Xinuos

OpenServer 10.3

RELEASE NOTES

About this release

OpenServer 10 (R3M0) is a new release of the OpenServer 10 operating system, which adds new features and includes security updates as well as enhancements in both **OpenSetup** and **OpenCommander**.

These release notes accompany this document:

OpenServer 10 GETTING STARTED GUIDE (January 2016)

available for free download at the Xinuos web site portal.

Contents of these Release Notes

What's New in this Release

General Enhancements

- UEFI boot loader now has classic boot menu.
  - Booting UEFI systems now present the same boot menu as the booting legacy BIOS systems does, so the same boot options are available.
- UEFI boot loader now supports booting ZFS root filesystems.
- Support for ZFS boot environments.
  - Boot loader will now show all existing boot environments of the root filesystem created from beadm.

- Added ZFSD (ZFS fault management daemon).
  - The backported version of ZFSD from FreeBSD 11 (yet to be released) has been added to this release.
- Linux emulation now supports 64bit and is based on CentOS Linux version 6.

OpenServer 10.3: Fixes and Enhancements

- Fixed: installer allowing to select the memory file system that the live DVD was using. (Note: memory file system still shows up on a USB install.)
- Fixed: The issue with tty.js has been resolved so that OpenSetup can run on R3M0 with node version 6.2.2.
- Updated: Based on reported problems, the minimum requirement for memory was changed from 2GB to 3GB.
- Updated: FreeBSD 10.3 updated OpenSSH to 7.2p2 which changed its default key fingerprint from md5 to sha256. Since most of the machines connecting will be older systems with only md5 fingerprint hash, we defaulted back to md5 to enhance the security of a first time connection. This is especially important for AWS with no console access.
- Added: ZFS fault management daemon (ZFSD).
- Added: variables to /etc/rc.conf (set to NO) for xrdp [ID: OSR10-433][1].
- Added: for AWS, /etc/ssh/sshd_config to keep connections up as long as wanted to work around overly aggressive firewall that drops ssh sessions before log out.

OpenSetup: Fixes and Enhancements

- Fixed: OpenSetup doesn't check for invalid hostname [ID: OSR10-449]
  - OpenSetup was not adequately checking the value of the "Set Hostname" parameter during installation and was allowing a comma in place of a period which would create an invalid Hostname.
- Fixed: LiveDVD Reporting [ID: OSR10-445]
  - An Internal Server Error message occurred when the user attempted to use the "Reporting" module of OpenCommander on LiveDVD.

[1] This and the following IDs refer to Xinuos internal tracking system.

- Fixed: OpenSetup Network settings [ID: OSR10-9]
  - When attempting to setup a static IP on the 2nd NIC, OpenSetup filled the field with the address for the first NIC. If the user edited the value and attempted to save it, it would fail with an error message, “Since you want to assign static IP to this adapter, please enter valid IP address and netmask.”
  - If automatic configuration (DHCP) was not selected, the domain field of /etc/resolv.conf was not filled in.
- Fixed: OpenSetup network issues [ID: OSR10-442]
  - Network values entered during installation were not being retained. Related to OSR10-436 below.
- Fixed: Network settings lost after first reboot [ID: OSR10-436]
  - Network settings (IP, netmask, etc.) entered during OpenSetup installation may not be retained after first re-boot and have to be entered manually afterward.
- Fixed: nginx config files are recreated at boot [ID: OSR10-434]
  - In /usr/local/etc/nginx, the files fastcgi_parms and nginx.conf were created new at each boot causing any local changes to be lost. Documented in the files that these files have been newly generated and the location of the master files.
- Fixed: missing variables in rc.conf [ID: OSR10-433]
  - rdp did not start by default after ISL and the variables were missing in /etc/rc.conf. These values have been added to /etc/rc.conf for DVD installs:

    ```
    xrdp_enable="NO"
    xrdp_sesman_enable="NO"
    ```
- Fixed: OpenSetup nic configuration [ID: OSR10-14]
  - System is not displaying all NICs that is has detected.
- Added: ZFS root on UEFI [ID: OSR10-404]
  - Has been added to OpenServer10.3

OpenCommander: Fixes and Enhancements

- The Xinuos stack solution allows Definitive Virtual Machines to run within OpenServer 10 (the "OSR10 Stack") so that companies can migrate Xinuos-based applications to a native environment in OpenServer 10 (see chapter OpenCommander and 'Definitive' Virtual Machines ("VM") on page 6 for detailed explanations).
- Fixed: alert doesn't report any network outage [ID: OSR10-52]
- Fixed: LiveDVD won't show any report with error message Internal Server Error [ID: OSR10-445]
- Fixed: when the license is expired, it doesn't display the generic OpenCommander error message [ID: OSR10-444]
- Fixed: nginx config files are recreated at boot [ID: OSR10-434]
- Fixed: OpenCommander alters mount points for ZFS pools [ID: OSR10-458]
- Fixed: Info message for Sysclt has a misspelling [ID: OSR10-460]
- Improved: OpenCommander network [ID: OSR10-11]
- Improved: screen layout/field size issues [ID: OSR10-380]
- Improved: detailed error message of the OSR10 Stack If no VM install [ID: OSR10-456]
- Improved: CPU Display [ID: OSR10-423]
- Improved Login error message [ID: OSR10-379]
- Improved: Disks display [ID: OSR10-422]
- Improved: storage module [ID: OSR10-16]
- Improved: MultiUser [ID: OSR10-399]
- Updated: support details [ID: OSR10-396]
- Added: Alert message should have the time and the date [ID: OSR10-459]
- Added: AutoLogout [ID: OSR10-402]

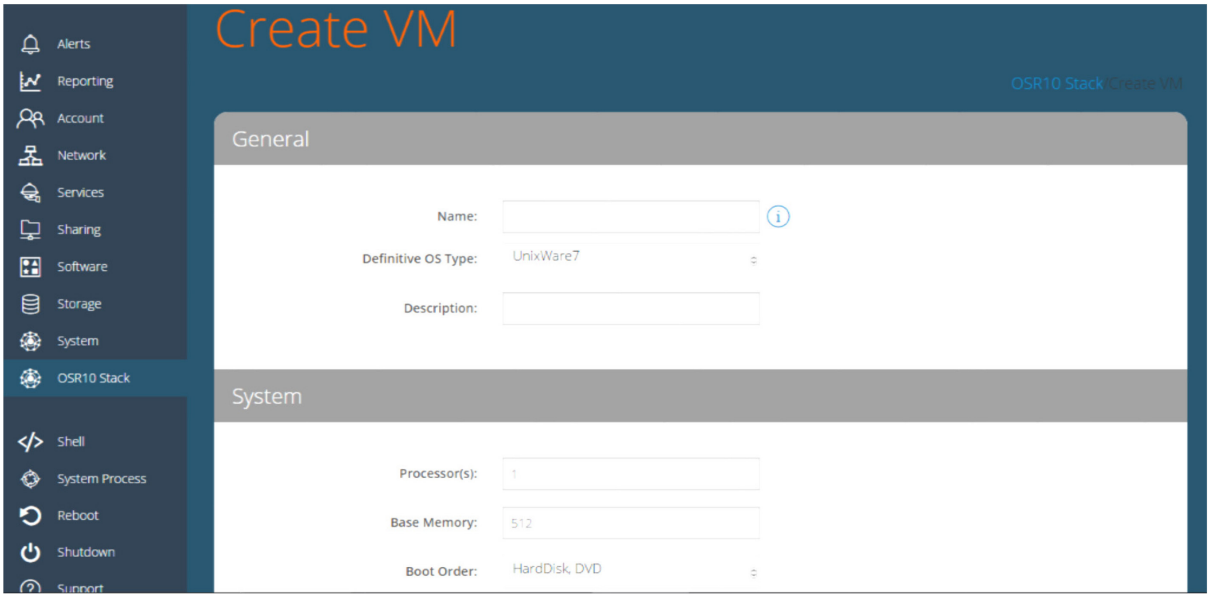
OpenCommander and 'Definitive' Virtual Machines ("VM")

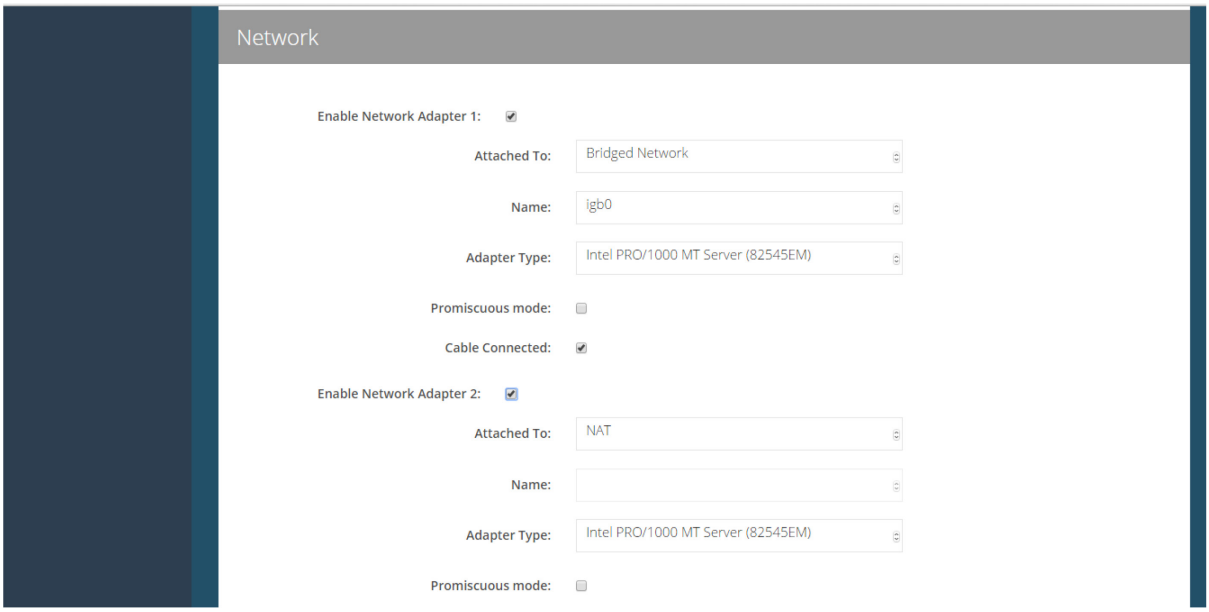
This functionality - The 'OSR10 Stack' module - is enabled on bare-metal systems only. It allows the Definitive versions of the other operating systems provided by Xinuos to run virtually on top of OpenServer 10.3.

Creation of VM in OpenCommander

UnixWare 7 Definitive will be used in this example.

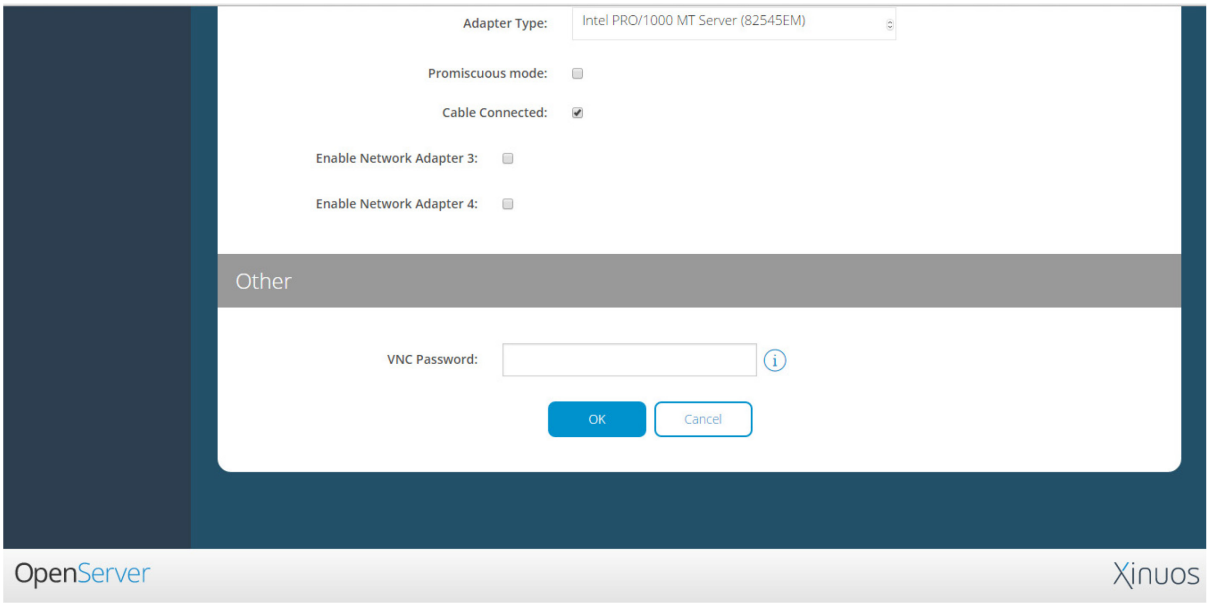
To create a new Definitive Virtual Machine, click on 'OSR10 Stack' module in OpenCommander and use the following 'Create VM' form:





- The following are the required fields:
  - Name: The name of virtual machine to create. This should be unique and should not be the same as any other existing virtual machine.
  - Definitive OS Type: Select the type of Definitive OS you are going to install on this virtual machine.
  - Processors & RAM: The default number of processor is 1 and RAM is 512MB. Please change these values as required.
  - Controller: Select a storage controller to be used. OpenServer507D works with only SATA controller.
  - Hard Disk File Size: Select a file size as per the Definitive OS being installed. The recommended file size for OpenServer is 8GB.
  - Optical Disk File: Select the Definitive ISO which will be used to install the Definitive OS on the virtual machine.
  - VNC Password: The password which will be used to access the virtual machine's console via VNC – Virtual Network Computing.

The first network adapter is enabled by default. Verify that the network settings are correct. These settings can be modified depending on the requirements of the virtual machine. If more than one network adapter is needed, select the checkbox to enable another network adapter and configure it as required.



Press 'OK' to create a new virtual machine.

Installation of 'Definitive' Operating System

When the above steps are completed and the virtual machine is created, it will be in the 'Powered Off' state. To start the installation of the Definitive OS on this virtual machine, select the virtual machine in the data-grid and press 'Start'. Once the machine is started, select 'Console' to connect to the virtual machine's console via VNC.

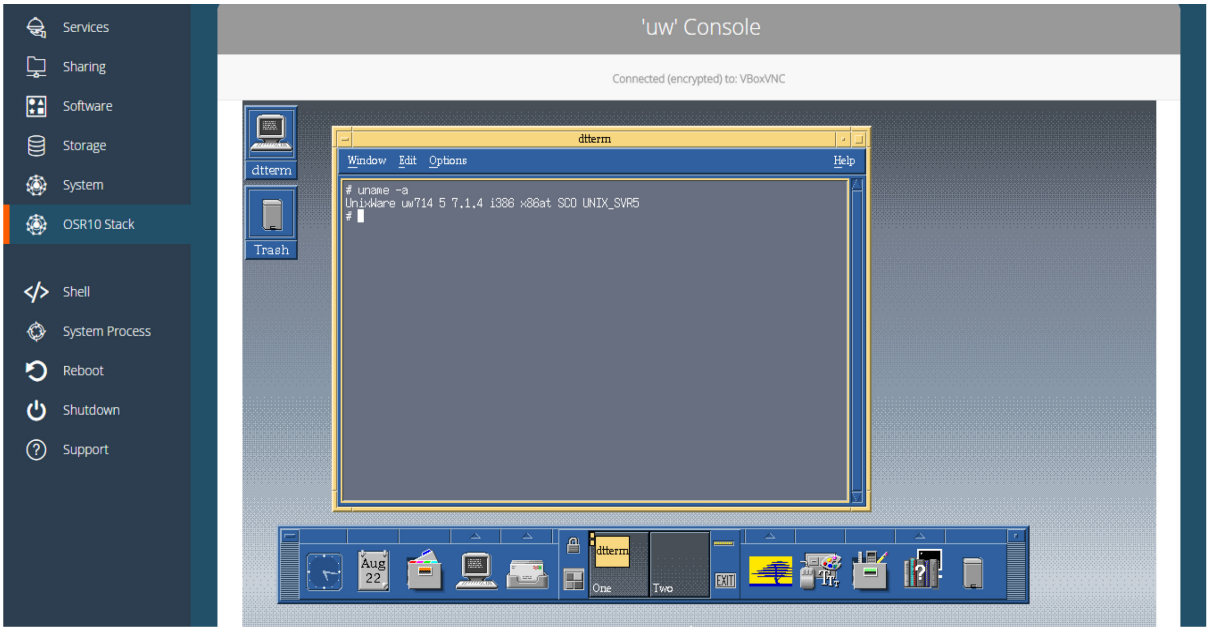
Follow the steps in the Definitive ISL (Initial Software Load) process to configure the installation. Once the installation is complete, UnixWare Definitive will display this screen:

Press the 'Eject CD' button to eject the Definitive ISO from the CD-ROM drive that is connected to the virtual machine. This screen is displayed:

If there is only one ISO connected to the virtual machine, it will be pre-selected. Press the 'Eject' button to eject the ISO.

Press enter on the console and virtual machine will reboot.

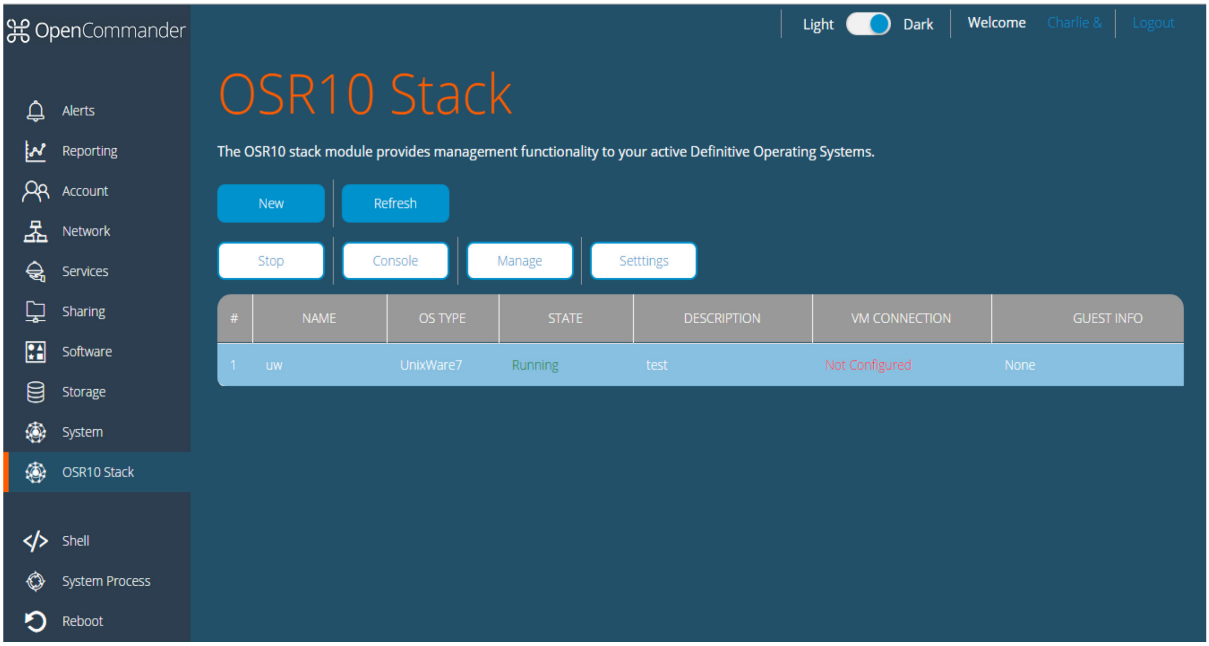
When the virtual machine boots successfully you will see a GUI console, if it was configured during ISL or a command prompt for login. Enter the login credentials that were used during ISL. After login, the following screen will display:



Modify Definitive VM

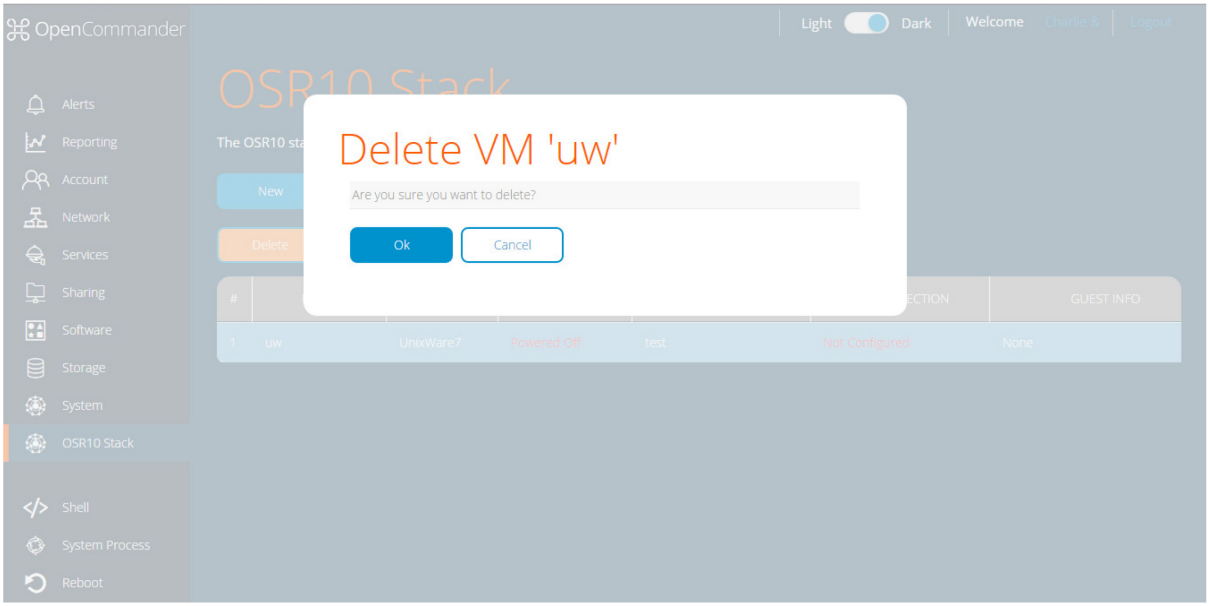
To modify a virtual machine's settings, select the virtual machine in the data-grid and press 'Settings'. This will open a form similar to 'Create VM' where you can modify the settings.

You can only modify the description and network settings if the virtual machine is currently running. To modify other settings please stop the virtual machine and then press the 'Settings' button.



Delete Definitive VM

To delete a virtual machine, it should be in stopped state. You can delete a virtual machine by selecting a virtual machine in the grid and press the 'Delete' button. If you also want to delete all the data for this virtual machine, select the checkbox in the confirmation prompt and press 'Ok'.



Stop Definitive VM

To use OpenCommander to stop a Virtual Machine, ensure that the VM has been shut down properly.

If you have entered the IP address & login credentials in 'Manage VM', you can stop the UnixWare Definitive VM using the OpenCommander User Interface.

To 'Stop' OpenServer6/Openserver5 Definitive, use the 'Console VM' tab in OpenCommander and issue the 'shutdown' command. When you see the "Press any key to reboot" message, use the 'Stop VM' button in the OpenCommander User Interface to stop/poweroff the VM.

VM Apps

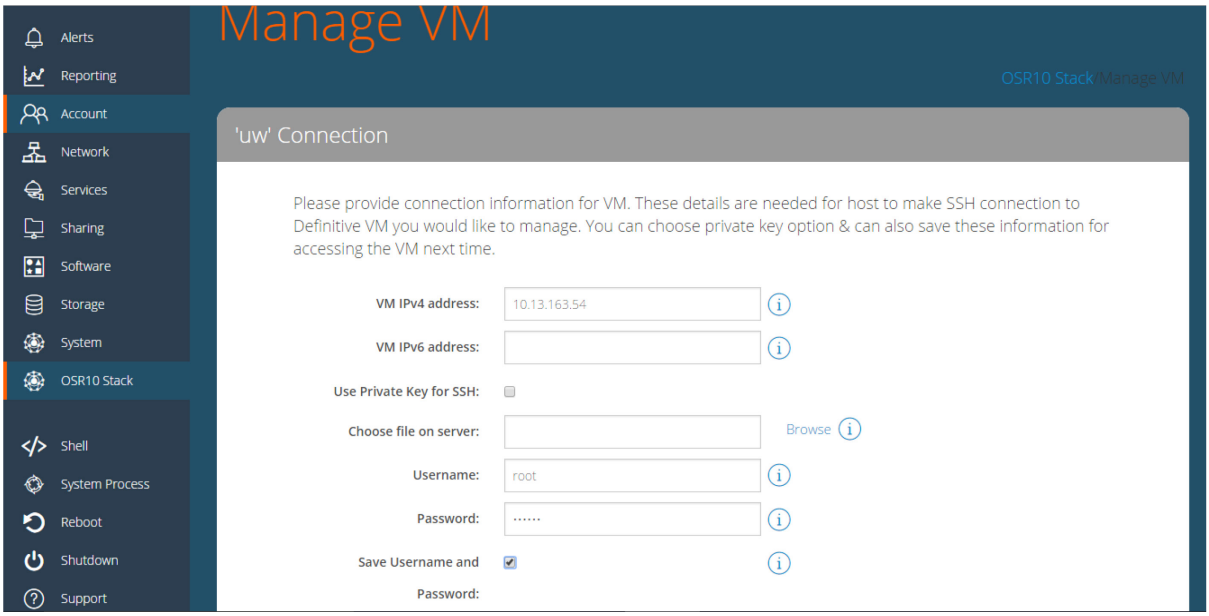
Users can manage a Definitive Virtual Machine via OpenCommander.

Create a new user on the Definitive OS. To enable management of the Virtual Machine, the user needs to provide the IP address assigned to the VM and the login credentials of the Definitive VM.

OpenCommander's password authentication can be used for connecting to the Definitive Virtual Machine. Provide the 'username' and 'password'.

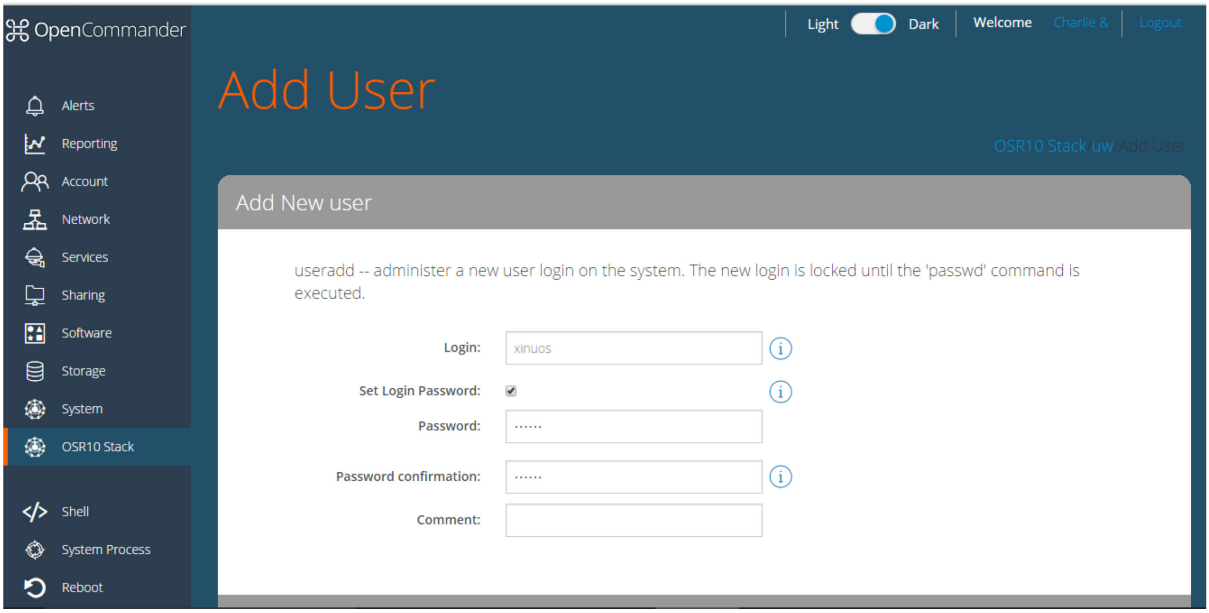
To use the private key authentication, select the checkbox 'Use private key for SSH' and select the private key to be used. This private key is stored in the OpenCommander database in an encrypted form.

If using the password authentication, the username and password can be saved in the OpenCommander database so that the user does not need to enter the credentials for this virtual machine every time a new session of OpenCommander is started. If you do not save the user name and password, the credentials will only work for the current session of OpenCommander that is active. Once the user logs out of the session, the credentials are no longer stored and available upon login. The user will have to enter these details again upon next login.



Add New User

When OpenCommander is able to connect with the Definitive virtual machine, a new user can be created on the Definitive OS by selecting 'Add new user'. To create a new user, fill the username, the password is optional, although if a password is not specified at this point, the new user will not be able to log into the Definitive OS.



Security Fixes

- Heap vulnerability in bspatch [ID: OSR10-471] -

  CVE Name: CVE-2014-9862

  - The implementation of bspatch does not check for a negative value on numbers of bytes read from the diff and extra streams, allowing an attacker who can control the patch file to write at arbitrary locations in the heap.
  - An attacker who can control the patch file can cause a crash or run arbitrary code under the credentials of the user who runs bspatch, in many cases, root.

- Multiple vulnerabilities of ntp [ID: OSR10-457]

  CVE Name: CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956

  - Multiple vulnerabilities have been discovered in the NTP suite.
  - The fix for Sec 3007 in ntp-4.2.8p7 contained a bug that could cause ntpd to crash. [CVE-2016-4957, Reported by Nicolas Edet of Cisco]
  - An attacker who knows the origin timestamp and can send a spoofed packet containing a CRYPTO-NAK to an ephemeral peer target before any other response is sent can demobilize that association. [CVE-2016-4953, Reported by Miroslav Lichvar of Redhat]
  - An attacker who is able to spoof packets with correct origin timestamps from enough servers before the expected response packets arrive at the target machine can affect some peer variables and, for example, cause a false leap indication to be set. [CVE-2016-4954, Reported by Jakub Prokes of Redhat]
  - An attacker who is able to spoof a packet with a correct origin timestamp before the expected response packet arrives at the target machine can send a CRYPTO_NAK or a bad MAC and cause the association's peer variables to be cleared. If this can be done often enough, it will prevent that association from working. [CVE-2016-4955, Reported by Miroslav Lichvar of Redhat]
  - The fix for NtpBug2978 does not cover broadcast associations, so broadcast clients can be triggered to flip into interleave mode. [CVE-2016-4956, Reported by Miroslav Lichvar of Redhat.]

- Malicious remote attackers may be able to break time synchronization, or cause the ntpd(8) daemon to crash.

► Directory traversal in cpio(1) [ID: OSR10-454]

CVE Name: CVE-2015-2304

- The cpio(1) tool from the libarchive(3) bundle is vulnerable to a directory traversal problem via absolute paths in an archive file. A malicious archive file being unpacked can overwrite an arbitrary file on a filesystem, if the owner of the cpio process has write access to it.

► Kernel Stack disclosure in 4.3BSD compatibility layer [ID: OSR10-453]

- The implementation of historic stat(2) system call does not clear the output struct before copying it out to userland.
- An unprivileged user can read a portion of uninitialised kernel stack data, which may contain sensitive information, such as the stack guard, portions of the file cache or terminal buffers, which an attacker might leverage to obtain elevated privileges.

► Kernel Stack disclosure in Linux compatibility layer [ID: OSR10-452]

- The implementation of the TIOCGSERIAL ioctl(2) does not clear the output struct before copying it out to userland.
- The implementation of the Linux sysinfo() system call does not clear the output struct before copying it out to userland.
- An unprivileged user can read a portion of uninitialised kernel stack data, which may contain sensitive information, such as the stack guard, portions of the file cache or terminal buffers, which an attacker might leverage to obtain elevated privileges.

► Incorrect argument handling in sendmsg(2) [ID: OSR10-451]

CVE Name: CVE-2016-1887

- Incorrect argument handling in the socket code allows malicious local user to overwrite large portion of the kernel memory.
- Malicious local user may crash kernel or execute arbitrary code in the kernel, potentially gaining superuser privileges.

► Buffer overflows in keyboard driver [ID: OSR10-450]

CVE Name: CVE-2016-1886

- Incorrect signedness comparison in the ioctl(2) handler allows a malicious local user to overwrite a portion of the kernel memory.
- A local user may crash the kernel, read a portion of kernel memory and execute arbitrary code in kernel context. The result of executing an arbitrary kernel code is privilege escalation.

► Multiple openssl vulnerabilities [ID: OSR10-447]

CVE Name: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176

- The padding check in AES-NI CBC MAC was rewritten to be in constant time by making sure that always the same bytes are read and compared against either the MAC or padding bytes. But it no longer checked that there was enough data to have both the MAC and padding bytes. [CVE-2016-2107]
- An overflow can occur in the EVP_EncodeUpdate() function which is used for Base64 encoding of binary data. [CVE-2016-2105]
- An overflow can occur in the EVP_EncryptUpdate() function, however it is believed that there can be no overflows in internal code due to this problem. [CVE-2016-2106]
- When ASN.1 data is read from a BIO using functions such as d2i_CMS_bio() a short invalid encoding can casuse allocation of large amounts of memory potentially consuming excessive resources or exhausting memory. [CVE-2016-2109]
- ASN1 Strings that are over 1024 bytes can cause an overread in applications using the X509_NAME_oneline() function on EBCDIC systems. [CVE-2016-2176] FreeBSD does not run on any EBCDIC systems and therefore is not affected.
- A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. [CVE-2016-2107]
- If an attacker is able to supply very large amounts of input data, a length check can overflow resulting in a heap corruption. [CVE-2016-2105]
- Any application parsing untrusted data through d2i BIO functions are vulnerable to memory exhaustion attack. [CVE-2016-2109] TLS applications are not affected.

► Multiple vulnerabilities of ntp [ID: OSR10-446]

CVE Name: CVE-2016-1547, CVE-2016-1548, CVE-2016-1549, CVE-2016-1550, CVE-2016-1551, CVE-2016-2516, CVE-2016-2517, CVE-2016-2518, CVE-2016-2519

- Multiple vulnerabilities have been discovered in the NTP suite:
- On OSes (FreeBSD not affected) that allows packets claiming to be from 127.0.0.0/8 that arrive over physical network, if ntpd is configured to use a reference clock, an attacker can inject packets over the network that look like they are coming from that reference clock. [CVE-2016-1551, Reported by Matt Street and others of Cisco ASIG]
- If a system is set up to use a trustedkey, and is not using the feature introduced in ntp-4.2.8p6 allowing an optional 4th field in the ntp.keys file to specify which IPs can serve time, a malicious authenticated peer, (i.e.; where the attacker knows the private symmetric key), can arbitrarily create many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock. [CVE-2016-1549, Reported by Matthew Van Gundy of Cisco ASIG]
- If ntpd was expressly configured to allow for remote configuration, (this is not common), a malicious user who knows the controlkey for ntpq or the requestkey for ntpdc (if mode7 is expressly enabled) can create a session with ntpd, and if an existing association is unconfigured using the same IP twice on the unconfig directive line, ntpd will abort. [CVE-2016-2516, Reported by Yihan Lian of the Cloud Security Team, Qihoo 360]
- If ntpd was expressly configured to allow for remote configuration (this is not common), a malicious user who knows the controlkey for ntpq or the requestkey for ntpdc (if mode7 is expressly enabled) can create a session with ntpd and then send a crafted packet to ntpd that will change the value of the trustedkey, controlkey, or requestkey to a value that will prevent any subsequent authentication with ntpd until ntpd is restarted. [CVE-2016-2517, Reported by Yihan Lian of the Cloud Security Team, Qihoo 360]
- Using a crafted packet to create a peer association with hmode > 7 causes the MATCH_ASSOC() lookup to make an out-of-bounds reference. [CVE-2016-2518, Reported by Yihan Lian of the Cloud Security Team, Qihoo 360]
- ntpq and ntpdc can be used to store and retrieve information in ntpd. It is possible to store a data value that is larger than the size of the buffer that the ctl_getitem() function of ntpd uses to report the return value. If the length of the requested data value returned by ctl_getitem() is too large, the value NULL is returned instead. There

are two cases where the return value from ctl_getitem() was not directly checked to make sure it is not NULL, but there are subsequent INSIST() checks that make sure the return value is not NULL. There are no data values ordinarily stored in ntpd that would exceed this buffer length, yet if a user has permission to store values and the user stores a value that is "too large", then ntpd will abort if an attempt is made to read that oversized value. [CVE-2016-2519, Reported by Yihan Lian of the Cloud Security Team, Qihoo 360]

- For ntp-4 versions, up to but not including ntp-4.2.8p7, an off-path attacker can cause a preemptable client association to be demobilized by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled. Furthermore, if the attacker keeps sending crypto NAK packets, for example one every second, the victim never has a chance to reestablish the association and synchronize time with that legitimate server. For ntp-4.2.8 up to ntp-4.2.8p6 there is less risk because more stringent checks are performed on incoming packets, but there are still ways to exploit this vulnerability in versions before ntp-4.2.8p7. [CVE-2016-1547, Reported by Stephen Gray and Matthew Van Gundy of Cisco ASIG]
- It is possible to change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode. An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. ntpq gives no indication that the mode has been switched. [CVE-2016-1548, Reported by Miroslav Lichvar of RedHat and separately by Jonathan Gardner of Cisco ASIG]
- Packet authentication tests have been performed using memcmp() or possibly bcmp(), and it is potentially possible for a local or perhaps LAN-based attacker to send a packet with an authentication payload and indirectly observe how much of the digest has matched. [CVE-2016-1550, Reported independently by Loganaden Velvindron, and Matthew Van Gundy and Stephen Gray of Cisco SIG]
- Malicious remote attackers may be able to break time synchornization, or cause the ntpd(8) daemon to crash.

► Incorrect argument validation in sysarch(2) [ID: OSR10-441]

CVE Name: CVE-2016-1885

- A special combination of sysarch(2) arguments specify a request to uninstall a set of descriptors from the LDT. The start descriptor is cleared and the number of descriptors are provided. Due to invalid use of a signed intermediate value in the bounds checking during argument validity verification, unbound zero'ing of the process LDT and adjacent memory can be initiated from usermode.
- This vulnerability could cause the kernel to panic. In addition, it is possible to perform a local Denial of Service against the system by unprivileged processes.

► OpenSSH xauth(1) command injection [ID: OSR10-440]

CVE Name: CVE-2016-3115

- Due to insufficient input validation in OpenSSH, a client which has permission to establish X11 forwarding sessions to a server can piggyback arbitrary shell commands on the data intended to be passed to the xauth tool.
- An attacker with valid credentials and permission to establish X11 forwarding sessions can bypass other restrictions which may have been placed on their account, for instance using ForceCommand directives in the server's configuration file.

► Multiple OpenSSL vulnerabilities [ID: OSR10-447]

CVE Name: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176

- The padding check in AES-NI CBC MAC was rewritten to be in constant time by making sure that always the same bytes are read and compared against either the MAC or padding bytes, although it no longer checked that there was enough data to have both the MAC and padding bytes. [CVE-2016-2107]
- An overflow can occur in the EVP_EncodeUpdate() function which is used for Base64 encoding of binary data. [CVE-2016-2105]
- An overflow can occur in the EVP_EncryptUpdate() function, however it is believed that there can be no overflows in internal code due to this problem. [CVE-2016-2106]
- When ASN.1 data is read from a BIO using functions such as d2i_CMS_bio() a short invalid encoding can cause allocation of large amounts of memory potentially consuming excessive resources or exhausting memory. [CVE-2016-2109]

- ASN1 Strings that are over 1024 bytes can cause an overread in applications using the X509_NAME_oneline() function on EBCDIC systems. [CVE-2016-2176] FreeBSD does not run on any EBCDIC systems and therefore is not affected.
- A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. [CVE-2016-2107]
- If an attacker is able to supply very large amounts of input data then a length check can overflow resulting in a heap corruption. [CVE-2016-2105]
- Any application parsing untrusted data through d2i BIO functions are vulnerable to memory exhaustion attack. [CVE-2016-2109] TLS applications are not affected.

► Multiple OpenSSL vulnerabilities [ID: OSR10-435]

CVE Name: CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800

- A cross-protocol attack was discovered that could lead to decryption of TLS sessions by using a server supporting SSLv2 and EXPORT cipher suites as a Bleichenbacher RSA padding oracle. Note that traffic between clients and non-vulnerable servers can be decrypted provided another server supporting SSLv2 and EXPORT ciphers, (even with a different protocol such as SMTP, IMAP or POP3), shares the RSA keys of the non-vulnerable server. This vulnerability is known as DROWN. [CVE-2016-0800]
- A double free bug was discovered when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources. This scenario is considered rare. [CVE-2016-0705]
- The SRP user database lookup method SRP_VBASE_get_by_user had confusing memory management semantics; the returned pointer was sometimes newly allocated, and sometimes owned by the callee. The calling code has no way of distinguishing these two cases. [CVE-2016-0798]
- In the BN_hex2bn function, the number of hex digits is calculated using an int value |i|. Later |bn_expand| is called with a value of |i * 4|. For large values of |i| this can result in |bn_expand| not allocating any memory because |i * 4| is negative. This can leave the internal BIGNUM data field as NULL leading to a subsequent NULL pointer dereference. For very large values of |i|, the calculation |i * 4| could be a positive value smaller than |i|. In this case memory is allocated to

the internal BIGNUM data field, but it is insufficiently sized leading to heap corruption. A similar issue exists in BN_dec2bn. This could have security consequences if BN_hex2bn/BN_dec2bn is ever called by user applications with very large untrusted hex/dec data. This is anticipated to be a rare occurrence. [CVE-2016-0797]

- The internal |fmtstr| function used in processing a "%s" formatted string in the BIO_*printf functions could overflow while calculating the length of a string and cause an out-of-bounds read when printing very long strings. [CVE-2016-0799]
- A side-channel attack was found which makes use of cache-bank conflicts on the Intel Sandy-Bridge microarchitecture which could lead to the recovery of RSA keys. [CVE-2016-0702]
- s2_srvr.c did not enforce that clear-key-length is 0 for non-export ciphers. If clear-key bytes are present for these ciphers, they displace encrypted-key bytes. [CVE-2016-0703]
- s2_srvr.c overwrites the wrong bytes in the master key when applying Bleichenbacher protection for export cipher suites. [CVE-2016-0704]
- Servers that have SSLv2 protocol enabled are vulnerable to the "DROWN" attack which allows a remote attacker to fast attack many recorded TLS connections made to the server, even when the client did not make any SSLv2 connections themselves.
- An attacker who can supply malformed DSA private keys to OpenSSL applications may be able to cause memory corruption which would lead to a Denial of Service condition. [CVE-2016-0705]
- An attacker connecting with an invalid username can cause memory leak, which could eventually lead to a Denial of Service condition. [CVE-2016-0798]
- An attacker who can inject malformed data into an application may be able to cause memory corruption which would lead to a Denial of Service condition. [CVE-2016-0797, CVE-2016-0799]
- A local attacker who has control of code in a thread running on the same hyper-threaded core as the victim thread which is performing decryptions could recover RSA keys. [CVE-2016-0702]
- An eavesdropper who can intercept SSLv2 handshake can conduct an efficient divide-and-conquer key recovery attack and use the server as an oracle to

determine the SSLv2 master-key, using only 16 connections to the server and negligible computation. [CVE-2016-0703]

- An attacker can use the Bleichenbacher oracle which enables a more efficient variant of the DROWN attack. [CVE-2016-0704]

64-Bit Linux Emulation Support

The Linux® compatibility layer has been substantially improved and now is capable of running 64-bit Linux applications on amd64 (x86_64), 1:1 threading, VDSO, and subset of the epoll(7) family sufficient for the majority of programs.

To achieve Linux emulation, one must have a Linux userland as well as a kernel, or in the case of FreeBSD, a binary interface. The emulators/linux_base-c6 is the base system of CentOS 6 and contains all the binaries and libraries needed to run Linux programs in FreeBSD. However, the port installs a 32-bit userland, which cannot be used for a 64-bit Linux application. Fortunately, this can be resolved by adding a few lines to /etc/make.conf:

```
OVERRIDE_LINUX_BASE_PORT=c6_64

OVERRIDE_LINUX_NONBASE_PORTS=c6_64
```

New and Updated Drivers

This section covers changes and additions to devices and device drivers since the 10.2-RELEASE.

Device Drivers

- The i.MX range is a family of Freescale Semiconductor (now part of NXP) proprietary microcontrollers for multimedia applications based on the ARM architecture. The ‘imxwdt’ driver, which supports Freescale i.MX watchdog, has been fixed by setting ‘WDOG_CR_WDE’ (enable bit) and error return values in certain situations now follow the rules from watchdog(9). This fix also enables the watchdog driver for IMX6.
- The ‘puc(4)’ (PCI Universal Communication) driver, which acts as a shim to connect PCI serial and parallel ports to the uart(4) and ppc(4) driver, now supports MSI interrupts

and prefers it to the legacy interrupts. This behaviour can be disabled by setting 'hw.puc.msi_disable' loader tunable. [r287926]

- The following fixes and modifications were made to the uart(4) driver.
  - A bug in the uart(4) driver which could cause a polarity reversal of PPS (Pulse Per Second) capture events has been fixed. The trailing edge of a positive PPS pulse and the leading edge of the next pulse were used as "assert" and "clear" event respectively.
  - The uart(4) driver now supports runtime configuration of PPS signal source captured by the driver dev.uart.pps_mode and dev.uart.0.pps_mode sysctl variables, eliminating the need to build a custom kernel to use the CTS signal.
  - The values 0, 1 and 2 correspond to disabled, capturing pulses on the CTS line, and capturing pulses on the DCD line, respectively. The default value is 2.
  - Document the change in polarity of the uart(4) PPS capture.
- The uftdi(4) driver now supports UFTDIIOC_READ_EEPROM, UFTDIIOC_WRITE_EEPROM, and UFTDIIOC_ERASE_EEPROM ioctl(2) to read/write serial EEPROM attached to the controller chip.

Storage Drivers

- Legacy ata(4) drivers such as ataahci, ataadaptec, and mv_sata have been removed in favour of the new drivers such as ahci(4), siis(4), and mvs(4). This removes about 3400 lines of code, unused since FreeBSD 9.0 release.
- The CTL (CAM Target Layer / iSCSI target) High Availability implementation has been rewritten. The CTL HA functionality was originally implemented by Copan many years ago, but a large part of the source was never published. This change includes clean room implementation of the missing code and fixes for many bugs.
- This code supports dual-node HA with ALUA in four modes:
  - Active/Unavailable without interlink between nodes;
  - Active/Standby with second node handling only basic LUN discovery and Reservation, synchronizing with the first node through the interlink;
  - Active/Active with both nodes processing commands and accessing the Backing storage, synchronizing with the first node through the interlink;

- Active/Active with second node working as proxy, transferring all Commands to the first node for execution through the interlink.

- Unlike Copan's original implementation, depending on specific hardware, this code uses simple custom TCP-based protocol for interlink. It has no authentication, so it should never be enabled on public interfaces.
- The ctl(4) driver has been updated to support CD-ROM and removable devices.
- The isp(4) driver has been updated and improved: added support for 16Gbps FC cards, improved target mode support, completed Multi-ID (NPIV) functionality.

The ctl(4) and isp(4) drivers are sponsored by iXsystems, Inc.

Network Drivers

- The following fixes and modification has been made to the ixgbe(4) driver.
  - Update ixgbe(4) to Intel FreeBSD Networking Group version 3.1.13-k. Added support for two new devices: X552 SFP+ 10 GbE, and the single port version of X550T.
  - Fix SFP module insertion post boot. Added PHY detection logic to ixgbe_handle_mod() and add locking to ixgbe_handle_msf() as well.
  - Fix VF handling of VLANs for Amazon Cloud. This helps immensely with our ability to operate in the Amazon Cloud.
- Firmware for model T4 and T5 bundled with the cxgbe(4) driver have been updated to version 1.14.4.0.

For fixes and enhancements to the firmare, please refer to:
https://svnweb.freebsd.org/base?view=revision&revision=286895

Hardware Support

This section covers general hardware support for physical machines, hypervisors, and virtualization environments, as well as hardware changes and updates that do not otherwise fit in other sections of this document.

- Hardware Support: The ismt(4) driver has been added, providing support for recent Intel® SMBus 2.0 controllers.
- Virtualization Support: The xen(4) driver has been updated to include support for blkif indirect segment I/O. This support is off by default in EC2 builds due to performance issues on some EC2 instance types.

Known Problems in this Release

OpenServer 10.3

- Unnecessary error message [OSR10-464]
  - On first re-boot after install, the message “Boot Failed: Windows boot Manager” may be seen and can be ignored. Also, the message “ ’S’ Not Found” may also be seen and can be ignored.
- ZFS failed message during reboot [OSR10-463]
  - When attempting a ZFS install, the following error messages may occur and can be ignored:

    "ZFS found the following pools ZFS1 ZFS Zroot"
    "ZFS I/O error all block copies unavailable"
    "Failed to read note from ZFS (5)"
- Unresponsive keyboard on ZFS configuration window [OSR10-462]
  - User needs to press “TAB” twice to use the keyboard on this window.

OpenCommander

- Keyboard is not available if VM console is connected. Please disconnect the VM console if you want to use keyboard in other modules.
- The caps lock key does NOT work when OSR10 Stack is connected to a VM console.
- Multiple console access is not supported. This happens when two OpenCommander sessions are using the same Definitive console.
- Double mouse pointer is visible in console window.
- If user has created a VM outside of OpenCommander and has not enabled VRDE, then user needs to run the following commands to enable console access from OpenCommander:

  # VBoxManage modifyvm <vm-name> --vrde on

  # VBoxManage modifyvm <vm-name> --vrdeport <vnc-port> (Always ensure that this port is unique and not used by any other VM)

  # VBoxManage modifyvm <vm-name> --vrdeproperty VNCPassword=somepass

- If a UnixWare VM is shutdown from the console, the grid will show the status of that machine as 'Stopping' and buttons to control the virtual machine will not be visible. To stop a UnixWare virtual machine, either use SSH or configure the virtual machine's credentials in Manage VM and use the Stop button to stop the virtual machine.
- Shutdown the OpenServer VM from OpenCommander console. Once you see the "Press any key to reboot" message, press the Stop VM button. If the virtual machine credentials are set in Manage VM and the 'Stop' button is pressed, the process will hang indefinitely
- The browse option in the Create VM/Modify VM screen sometimes does not work. If this happens, refresh the browser tab and the option will start working again.

Security and Errata

This section lists the various Security Advisories and Errata Notices since the 10.2-RELEASE:

- FreeBSD-SA-16:03.linux: Linux compatibility layer incorrect futex handling may result in incorrect memory locations being accessed.
- FreeBSD-SA-16:04.linux: Linux compatibility layer setgroups(2) system call vulnerability can lead to unexpected results, such as overwriting random kernel memory contents.
- FreeBSD-SA-16:10.linux: Linux compatibility layer issetugid(2) system call vulnerability could cause the issetugid(2) system call to return incorrect information.

Addendum – Release Notes of FreeBSD 10.3

OpenServer 10.3 is based on FreeBSD 10.3.

To complete the list of all changes, a copy of the FreeBSD 10.3 release notes is included here for your convenience:

10.3-RELEASE Release Notes

The FreeBSD Project

Last modified on 2016-03-25 by gjb.

Abstract

The release notes for FreeBSD 10.3-RELEASE contain a summary of the changes made to the FreeBSD base system on the 10.3-STABLE development line. This document lists applicable security advisories that were issued since the last release, as well as significant changes to the FreeBSD kernel and userland. Some brief remarks on upgrading are also presented.

Table of Contents

1. Introduction

This document contains the release notes for FreeBSD 10.3-RELEASE. It describes recently added, changed, or deleted features of FreeBSD. It also provides some notes on upgrading from previous versions of FreeBSD.

The snapshot distribution to which these release notes apply represents a point along the 10.3-STABLE

development branch between 10.2-RELEASE and the future 10.4-RELEASE. Information regarding pre-built, binary snapshot distributions along this branch can be found at https://www.FreeBSD.org/releases/.

All users are encouraged to consult the release errata before installing FreeBSD. The errata document is updated with “late-breaking” information discovered late in the release cycle or after the release. Typically, it contains information on known bugs, security advisories, and corrections to documentation. An up-to-date copy of the errata for FreeBSD 10.3-RELEASE can be found on the FreeBSD Web site.

This document describes the most user-visible new or changed features in FreeBSD since 10.2-RELEASE.

Typical release note items document recent security advisories issued after 10.2-RELEASE, new drivers or hardware support, new commands or options, major bug fixes, or contributed software upgrades. They may also list changes to major ports/packages or release engineering practices. Clearly the release notes cannot list every single change made to FreeBSD between releases; this document focuses primarily on security advisories, user-visible changes, and major architectural improvements.

2. Upgrading from Previous Releases of FreeBSD

[amd64,i386] Binary upgrades between RELEASE versions (and snapshots of the various security branches) are supported using the freebsd-update(8) utility. The binary upgrade procedure will update unmodified userland utilities, as well as unmodified GENERIC kernel distributed as a part of an official FreeBSD release. The freebsd-update(8) utility requires that the host being upgraded have Internet connectivity.

Source-based upgrades (those based on recompiling the FreeBSD base system from source code) from previous versions are supported, according to the instructions in /usr/src/UPDATING.

Important:

Upgrading FreeBSD should only be attempted after backing up all data and configuration files.

3. Security and Errata

This section lists the various Security Advisories and Errata Notices since 10.2-RELEASE.

3.1. Security Advisories

Advisory Date Topic

FreeBSD-SA-15:20.expat 18 August 2015

Topic: Multiple integer overflows in expat (libbsdxml) XML parser
Category: contrib
Module: libbsdxml
Announced: 2015-08-18

Affects: All supported versions of FreeBSD.
Corrected: 2015-08-18 19:30:05 UTC (stable/10, 10.2-STABLE)
2015-08-18 19:30:35 UTC (releng/10.1, 10.1-RELEASE-p18)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RC3-p1)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RELEASE-p1)
2015-08-18 19:30:05 UTC (stable/9, 9.3-STABLE)
2015-08-18 19:30:35 UTC (releng/9.3, 9.3-RELEASE-p23)
CVE Name: CVE-2015-1283
For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

Expat is an XML parser library written in C. It is a stream-oriented parser in which an application registers handlers for things the parser might find in the XML document (like start tags).

The FreeBSD base system ships libexpat as libbsdxml for components that need to parse XML data. Some of these applications use the XML parser on trusted data from the kernel, for instance the geom(8) configuration utilities, while other applications, like tar(1), cpio(1), svnlite(1) and unbound-anchor(8), may use the XML parser on input from network or the user.

II. Problem Description

Multiple integer overflows have been discovered in the XML_GetBuffer() function in the expat library.

III. Impact

The integer overflows may be exploited by using specifically crafted XML data and lead to infinite loop, or a heap buffer overflow, which results in a Denial of Service condition, or enables remote attackers to execute arbitrary code.

Fix multiple integer overflows in libbsdxml(3).

FreeBSD-SA-15:22.openssh 25 August 2015

Topic: OpenSSH multiple vulnerabilities

Category: contrib
Module: openssh
Announced: 2015-08-25
Affects: All supported versions of FreeBSD.
Corrected: 2015-08-25 20:48:44 UTC (stable/10, 10.2-STABLE)

2015-08-25 20:48:51 UTC (releng/10.2, 10.2-RC3-p2)
2015-08-25 20:48:51 UTC (releng/10.2, 10.2-RELEASE-p2)
2015-08-25 20:48:58 UTC (releng/10.1, 10.1-RELEASE-p19)
2015-08-25 20:48:44 UTC (stable/9, 9.3-STABLE)
2015-08-25 20:49:05 UTC (releng/9.3, 9.3-RELEASE-p24)

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

OpenSSH is an implementation of the SSH protocol suite, providing an encrypted and authenticated transport for a variety of services, including remote shell access.

The PAM (Pluggable Authentication Modules) library provides a flexible framework for user authentication and session setup / teardown.

The default FreeBSD OpenSSH configuration has PAM interactive authentication enabled.

Privilege separation is a technique in which a program is divided into multiple cooperating processes, each with a different task, where each process is limited to the specific privileges required to perform that specific task, while the privileged parent process acts as an arbiter.

II. Problem Description

A programming error in the privileged monitor process of the sshd(8) service may allow the username of an already-authenticated user to be overwritten by the unprivileged child process.

A use-after-free error in the privileged monitor process of he sshd(8) service may be deterministically triggered by the actions of a compromised unprivileged child process.

A use-after-free error in the session multiplexing code in the sshd(8) service may result in unintended termination of the connection.

III. Impact

The first bug may allow a remote attacker who a) has already succeeded by other means in compromising the unprivileged pre-authentication child process and b) has valid credentials to one user on the target system to impersonate a different user.

The second bug may allow a remote attacker who has already succeeded by other means in compromising the unprivileged pre-authentication child process to bypass PAM authentication entirely.

The third bug is not exploitable, but can cause premature termination of a multiplexed ssh connection.

Multiple vulnerabilities

FreeBSD-SA-15:24.rpcbind 29 September 2015

Topic: rpcbind(8) remote denial of service [REVISED]

Category: core
Module: rpcbind
Announced: 2015-09-29, revised on 2015-10-02
Affects: All supported versions of FreeBSD.
Corrected: 2015-10-02 16:36:16 UTC (stable/10, 10.2-STABLE)
2015-10-02 16:37:06 UTC (releng/10.2, 10.2-RELEASE-p5)
2015-10-02 16:37:06 UTC (releng/10.1, 10.1-RELEASE-p22)
2015-10-02 16:36:16 UTC (stable/9, 9.3-STABLE)
2015-10-02 16:37:06 UTC (releng/9.3, 9.3-RELEASE-p28)
CVE Name: CVE-2015-7236

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

0. Revision history

v1.0 2015-09-29 Initial release.
v1.1 2015-10-02 Revised patch to address a regression related to NIS usage

I. Background

Sun RPC is a remote procedure call framework which allows clients to invoke procedures in a server process over a network transparently.

The rpcbind(8) utility is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine.

The Sun RPC framework uses a netbuf structure to represent the transport specific form of a universal transport address. The structure is expected to be opaque to consumers. In the current implementation, the structure contains a pointer to a buffer that holds the actual address.

II. Problem Description

In rpcbind(8), netbuf structures are copied directly, which would result in two netbuf structures that reference to one shared address buffer. When one of the two netbuf structures is freed, access to the other netbuf structure would result in an undefined result that may crash the rpcbind(8) daemon.

III. Impact

A remote attacker who can send specifically crafted packets to the rpcbind(8) daemon can cause it to crash, resulting in a denial of service condition.

IV. Workaround

No workaround is available, but systems that do not provide the rpcbind(8) service to untrusted systems, or do not provide any RPC services are not vulnerable. On FreeBSD, typical RPC based services includes NIS and NFS.

Alternatively, rpcbind(8) can be configured to bind on specific IP address(es) by using the '-h' option. This may be used to reduce the attack vector when the system has multiple network interfaces and when some of them would face an untrusted network.

Remote denial of service

FreeBSD-SA-15:25.ntp 26 October 2015

Topic: Multiple vulnerabilities of ntp [REVISED]

Category: contrib
Module: ntp
Announced: 2015-10-26, revised on 2015-11-04
Credits: Network Time Foundation
Affects: All supported versions of FreeBSD.
Corrected: 2015-10-26 11:35:40 UTC (stable/10, 10.2-STABLE)
2015-11-04 11:27:13 UTC (releng/10.2, 10.2-RELEASE-p7)
2015-11-04 11:27:21 UTC (releng/10.1, 10.1-RELEASE-p24)
2015-11-02 10:39:26 UTC (stable/9, 9.3-STABLE)
2015-11-04 11:27:30 UTC (releng/9.3, 9.3-RELEASE-p30)
CVE Name: CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855, CVE-2015-7871

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit https://security.FreeBSD.org/.

0. Revision history.

v1.0 2015-10-26 Initial release.
v1.1 2015-11-04 Revised patches to address regression in ntpq(8), ntpdc(8) utilities and lack of RAWDCF reference clock support in ntpd(8).

I. Background

The ntpd(8) daemon is an implementation of the Network Time Protocol (NTP) used to synchronize the time of a computer system to a reference time source.

II. Problem Description

Crypto-NAK packets can be used to cause ntpd(8) to accept time from an unauthenticated ephemeral symmetric peer by bypassing the authentication required to mobilize peer associations. [CVE-2015-7871]
FreeBSD 9.3 and 10.1 are not affected.

If ntpd(8) is fed a crafted mode 6 or mode 7 packet containing an unusually long data value where a network address is expected, the decodenetnum() function will abort with an assertion failure instead of simply returning a failure condition. [CVE-2015-7855]

If ntpd(8) is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd(8) was configured to disable authentication, then an attacker can send a set of packets to ntpd(8) that may cause it to crash, with the hypothetical possibility of a small code injection. [CVE-2015-7854]

A negative value for the datalen parameter will overflow a data buffer. The NTF ntpd(8) driver implementation always sets this value to 0 and are therefore not vulnerable to this weakness. If the system runs a custom refclock driver in ntpd(8) and that driver supplies a negative value for datalen (no custom driver of even minimal competence would do this), then ntpd(8) would overflow the data buffer. It is even hypothetically possible in this case that instead of simply crashing ntpd(8), the attacker could effect a code injection attack. [CVE-2015-7853]

If an attacker can figure out the precise moment that ntpq(8) is listening for data and the port number on which it is listening, or if the attacker can provide a malicious instance ntpd(8) that victims will connect to, then an attacker can send a set of crafted mode 6 response packets that, if received by ntpq(8), can cause ntpq(8) to crash. [CVE-2015-7852]

If ntpd(8) is configured to allow remote configuration, and if the (possibly spoofed) IP address is allowed to send remote configuration requests, and if

the attacker knows the remote configuration password or if ntpd(8) was configured to disable authentication, then an attacker can send a set of packets to ntpd that may cause ntpd(8) to overwrite files. [CVE-2015-7851]
The default configuration of ntpd(8) within FreeBSD does not allow remote configuration.

If ntpd(8) is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd(8) was configured to disable authentication, then an attacker can send a set of packets to ntpd that will cause it to crash and/or create a potentially huge log file. Specifically, the attacker could enable extended logging, point the key file at the log file, and cause what amounts to an infinite loop. [CVE-2015-7850]
The default configuration of ntpd(8) within FreeBSD does not allow remote configuration.

If ntpd(8) is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd(8) was configured to disable authentication, then an attacker can send a set of packets to ntpd(8) that may cause a crash or theoretically perform a code injection attack. [CVE-2015-7849]
The default configuration of ntpd(8) within FreeBSD does not allow remote configuration.

If ntpd(8) is configured to enable mode 7 packets, and if the use of mode 7 packets is not properly protected through the use of the available mode 7 authentication and restriction mechanisms, and if the (possibly spoofed) source IP address is allowed to send mode 7 queries, then an attacker can send a crafted packet to ntpd that will cause it to crash. [CVE-2015-7848]
The default configuration of ntpd(8) within FreeBSD does not allow mode 7 packets.

If ntpd(8) is configured to use autokey, then an attacker can send packets to ntpd that will, after several days of ongoing attack, cause it to run out of memory. [CVE-2015-7701]
The default configuration of ntpd(8) within FreeBSD does not use autokey.

If ntpd(8) is configured to allow for remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password, it is possible for an attacker to use the "pidfile" or "driftfile" directives to potentially overwrite other files. [CVE-2015-5196]
The default configuration of ntpd(8) within FreeBSD does not allow remote configuration

An ntpd(8) client that honors Kiss-of-Death responses will honor Kiss-of-Death messages that have been forged by an attacker, causing it to delay or stop querying its servers for time updates. Also, an attacker can forge packets that claim to be from the target and send them to servers often enough that a server that implements Kiss-of-Death rate limiting will send the target machine a Kiss-of-Death response to attempt to reduce the rate of incoming packets, or it may also trigger a firewall block at the server for packets from the target machine. For either of these attacks to succeed, the attacker must know what servers the target is communicating with. An attacker can be anywhere on the Internet and can frequently learn the identity of the time source of a target by sending the target a time query. [CVE-2015-7704]

The fix for CVE-2014-9750 was incomplete in that there were certain code paths where a packet with particular autokey operations that contained malicious data was not always being completely validated. Receipt of these packets can cause ntpd to crash. [CVE-2015-7702].
The default configuration of ntpd(8) within FreeBSD does not use autokey.

III. Impact

An attacker which can send NTP packets to ntpd(8) which uses cryptographic authentication of NTP data, may be able to inject malicious time data causing the system clock to be set incorrectly. [CVE-2015-7871]

An attacker which can send NTP packets to ntpd(8) can block the communication of the daemon with time servers, causing the system clock not being synchronized. [CVE-2015-7704]

An attacker which can send NTP packets to ntpd(8) can remotely crash the daemon, sending malicious data packet. [CVE-2015-7855] [CVE-2015-7854] [CVE-2015-7853] [CVE-2015-7852] [CVE-2015-7849] [CVE-2015-7848]

An attacker which can send NTP packets to ntpd(8) can remotely trigger the daemon to overwrite its configuration files. [CVE-2015-7851] [CVE-2015-5196]

Multiple vulnerabilities

FreeBSD-SA-15:26.openssl 5 December 2015

Topic: Multiple OpenSSL vulnerabilities

Category: contrib
Module: openssl
Announced: 2015-12-05
Affects: All supported versions of FreeBSD.
Corrected: 2015-12-03 21:18:48 UTC (stable/10, 10.2-STABLE)
2015-12-05 09:53:58 UTC (releng/10.2, 10.2-RELEASE-p8)

2015-12-05 09:53:58 UTC (releng/10.1, 10.1-RELEASE-p25)
2015-12-03 21:24:40 UTC (stable/9, 9.3-STABLE)
2015-12-05 09:53:58 UTC (releng/9.3, 9.3-RELEASE-p31)
CVE Name: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

FreeBSD includes software from the OpenSSL Project. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

II. Problem Description

The signature verification routines will crash with a NULL pointer dereference if presented with an ASN.1 signature using the RSA PSS algorithm and absent mask generation function parameter. [CVE-2015-3194]

When presented with a malformed X509_ATTRIBUTE structure, OpenSSL will leak memory. [CVE-2015-3195]

If PSK identity hints are received by a multi-threaded client then the values are incorrectly updated in the parent SSL_CTX structure. [CVE-2015-3196]

III. Impact

A remote attacker who can present a specifically crafted certificate may cause a OpenSSL client or server application that performs certificate signature verification to crash with a NULL pointer dereference, resulting in a Denial of Service. [CVE-2015-3194] This affects FreeBSD 10.x only.

An attacker who is able to feed specifically crafted PKCS#7/CMS data to an OpenSSL application can cause memory leak which may eventually result in a Denial of Service. [CVE-2015-3195]

A remote attacker who can send PSK identity hints to a multi-thread client may trigger a double fault of hint data, which may lead to crash the client application. [CVE-2015-3196]. This affects FreeBSD 10.1 only.

Multiple vulnerabilities

FreeBSD-SA-16:01.sctp 14 January 2016

Topic: SCTP ICMPv6 error message vulnerability

Category: core
Module: SCTP
Announced: 2016-01-14
Credits: Jonathan T. Looney
Affects: All supported versions of FreeBSD
Corrected: 2016-01-14 09:11:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-14 09:11:48 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2016-1879

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The Stream Control Transmission Protocol (SCTP) protocol provides reliable, flow-controlled, two-way transmission of data.

The Internet Control Message Protocol for IPv6 (ICMPv6) provides a way for hosts on the Internet to exchange control information. Among other uses, a host or router can use ICMPv6 to inform a host when there is an error delivering a packet sent by that host.

II. Problem Description

A lack of proper input checks in the ICMPv6 processing in the SCTP stack can lead to either a failed kernel assertion or to a NULL pointer dereference. In either case, a kernel panic will follow.

III. Impact

A remote, unauthenticated attacker can reliably trigger a kernel panic in a vulnerable system running IPv6. Any kernel compiled with both IPv6 and SCTP support is vulnerable. There is no requirement to have an SCTP socket open.

IPv4 ICMP processing is not impacted by this vulnerability.
ICMPv6 error message vulnerability

FreeBSD-SA-16:02.ntp 14 January 2016

Topic: ntp panic threshold bypass vulnerability

Category: contrib
Module: ntp
Announced: 2016-01-14
Credits: Network Time Foundation
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-11 01:09:50 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-11 01:48:16 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2015-5300

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The ntpd(8) daemon is an implementation of the Network Time Protocol (NTP) used to synchronize the time of a computer system to a reference time source.

II. Problem Description

The ntpd(8) daemon has a safety feature to prevent excessive stepping of the clock called the "panic threshold". If ever ntpd(8) determines the system clock is incorrect by more than this threshold, the daemon exits. There is an implementation error within the ntpd(8) implementation of this feature, which allows the system time be adjusted in certain circumstances.

III. Impact

When ntpd(8) is started with the '-g' option specified, the system time will be corrected regardless of if the time offset exceeds the panic threshold (by default, 1000 seconds). The FreeBSD rc(8) subsystem allows specifying the '-g' option by either including '-g' in the ntpd_flags list or by enabling ntpd_sync_on_start in the system rc.conf(5) file.

If at the moment ntpd(8) is restarted, an attacker can immediately respond to enough requests from enough sources trusted by the target, which is difficult and not common, there is a window of opportunity where the attacker can cause ntpd(8) to set the time to an arbitrary value.
Panic threshold bypass vulnerability

FreeBSD-SA-16:03.linux14 January 2016

Topic: Linux compatibility layer incorrect futex handling

Category: core
Module: kernel
Announced: 2016-01-14
Credits: Mateusz Guzik
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-14 09:11:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-14 09:11:48 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2016-1880

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:http://security.FreeBSD.org/>.

I. Background

FreeBSD is binary-compatible with the Linux operating system through a loadable kernel module/optional kernel component. The support is provided on amd64 and i386 machines.

II. Problem Description

A programming error in the handling of Linux futex robust lists may result in incorrect memory locations being accessed.

III. Impact

It is possible for a local attacker to read portions of kernel memory, which may result in a privilege escalation.
Incorrect futex handling

FreeBSD-SA-16:04.linux14 January 2016

Topic: Linux compatibility layer setgroups(2) system call vulnerability

Category: core
Module: kernel
Announced: 2016-01-14
Credits: Dmitry Chagin
Affects: All supported versions of FreeBSD
Corrected: 2016-01-14 09:11:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)

2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-14 09:11:48 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2016-1881

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

FreeBSD is binary-compatible with the Linux operating system through a loadable kernel module/optional kernel component. The support is provided on amd64 and i386 machines.

II. Problem Description

A programming error in the Linux compatibility layer setgroups(2) system call can lead to an unexpected results, such as overwriting random kernel memory contents.

III. Impact

It is possible for a local attacker to overwrite portions of kernel memory, which may result in a privilege escalation or cause a system panic.

setgroups(2) system call vulnerability

FreeBSD-SA-16:05.tcp 14 January 2016

Topic: TCP MD5 signature denial of service

Category: core
Module: kernel
Announced: 2016-01-14
Credits: Ryan Stone,
Jonathan T. Looney
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-14 09:11:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-14 09:11:48 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2016-1882

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the

following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The Transmission Control Protocol (TCP) of the TCP/IP protocol suite provides a connection-oriented, reliable, sequence-preserving data stream service. An optional extension to TCP described in RFC 2385 allows protecting data streams against spoofed packets with MD5 signature.

Support for TCP MD5 signatures is not enabled in default kernel.

II. Problem Description

A programming error in processing a TCP connection with both TCP_MD5SIG and TCP_NOOPT socket options may lead to kernel crash.

III. Impact

A local attacker can crash the kernel, resulting in a denial-of-service.

A remote attack is theoretically possible, if server has a listening socket with TCP_NOOPT set, and server is either out of SYN cache entries, or SYN cache is disabled by configuration.

MD5 signature denial of service

FreeBSD-SA-16:06.bsnmpd 14 January 2016

Topic: Insecure default snmpd.config permissions

Category: contrib
Module: bsnmpd
Announced: 2016-01-14
Credits: Pierre Kim
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-14 09:11:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-14 09:11:48 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)
CVE Name: CVE-2015-5677

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The bsnmpd daemon serves the Internet SNMP (Simple Network Management Protocol). It is intended to serve only the absolute basic MIBs and implements all other MIBs through loadable modules.

II. Problem Description

The SNMP protocol supports an authentication model called USM, which relies on a shared secret. The default permission of the snmpd.configiguration file, /etc/snmpd.config, is weak and does not provide adequate protection against local unprivileged users.

III. Impact

A local user may be able to read the shared secret, if configured and used by the system administrator.

Insecure default configuration file permissions

FreeBSD-SA-16:07.openssh 14 January 2016

Topic: OpenSSH client information leak

Category: contrib
Module: openssh
Announced: 2016-01-14
Credits: Qualys Security Advisory Team
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-14 22:42:43 UTC (stable/10, 10.2-STABLE)
2016-01-14 22:45:33 UTC (releng/10.2, 10.2-RELEASE-p10)
2016-01-14 22:47:54 UTC (releng/10.1, 10.1-RELEASE-p27)
2016-01-14 22:50:35 UTC (stable/9, 9.3-STABLE)
2016-01-14 22:53:07 UTC (releng/9.3, 9.3-RELEASE-p34)
CVE Name: CVE-2016-0777

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

OpenSSH is an implementation of the SSH protocol suite, providing an encrypted and authenticated transport for a variety of services, including remote shell access. The ssh(1) is client side utility used to login to remote servers.

II. Problem Description

The OpenSSH client code contains experimental support for resuming SSH

connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys.

III. Impact

A user that authenticates to a malicious or compromised server may reveal private data, including the private SSH key of the user.

OpenSSH client information leak

FreeBSD-SA-16:09.ntp 27 January 2016

Topic: Multiple vulnerabilities of ntp

Category: contrib
Module: ntp
Announced: 2016-01-27
Credits: Cisco ASIG / Network Time Foundation
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-22 15:55:21 UTC (stable/10, 10.2-STABLE)
2016-01-27 07:41:31 UTC (releng/10.2, 10.2-RELEASE-p11)
2016-01-27 07:41:31 UTC (releng/10.1, 10.1-RELEASE-p28)
2016-01-22 15:56:35 UTC (stable/9, 9.3-STABLE)
2016-01-27 07:42:11 UTC (releng/9.3, 9.3-RELEASE-p35)
CVE Name: CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The ntpd(8) daemon is an implementation of the Network Time Protocol (NTP) used to synchronize the time of a computer system to a reference time source.

II. Problem Description

Multiple vulnerabilities have been discovered in ntp 4.2.8p5:

Potential Infinite Loop in ntpq. [CVE-2015-8158]

A logic error would allow packets with an origin timestamp of zero to bypass this check whenever there is not an outstanding request

to the server. [CVE-2015-8138]

Off-path Denial of Service (DoS) attack on authenticated broadcast mode. [CVE-2015-7979]

Stack exhaustion in recursive traversal of restriction list. [CVE-2015-7978]

reslist NULL pointer dereference. [CVE-2015-7977]

ntpq saveconfig command allows dangerous characters in filenames. [CVE-2015-7976]

nextvar() missing length check. [CVE-2015-7975]

Skeleton Key: Missing key check allows impersonation between authenticated peers. [CVE-2015-7974]

Deja Vu: Replay attack on authenticated broadcast mode. [CVE-2015-7973]

ntpq vulnerable to replay attacks. [CVE-2015-8140]

Origin Leak: ntpq and ntpdc, disclose origin. [CVE-2015-8139]

III. Impact

A malicious NTP server, or an attacker who can conduct MITM attack by intercepting NTP query traffic, may be able to cause a ntpq client to infinitely loop. [CVE-2015-8158]

A malicious NTP server, or an attacker who can conduct MITM attack by intercepting NTP query traffic, may be able to prevent a ntpd(8) daemon to distinguish between legitimate peer responses from forgeries. This can partially be mitigated by configuring multiple time sources. [CVE-2015-8138]

An off-path attacker who can send broadcast packets with bad authentication (wrong key, mismatched key, incorrect MAC, etc) to broadcast clients can cause these clients to tear down associations. [CVE-2015-7979]

An attacker who can send unauthenticated 'reslist' command to a NTP server may cause it to crash, resulting in a denial of service condition due to stack exhaustion [CVE-2015-7978] or a NULL pointer dereference [CVE-2015-7977].

An attacker who can send 'modify' requests to a NTP server may be able to create file that contain dangerous characters in their name,

which could cause dangerous behavior in a later shell invocation. [CVE-2015-7976]

A remote attacker may be able to crash a ntpq client. [CVE-2015-7975]

A malicious server which holds a trusted key may be able to impersonate other trusted servers in an authenticated configuration. [CVE-2015-7974]

A man-in-the-middle attacker or a malicious participant that has the same trusted keys as the victim can replay time packets if the NTP network is configured for broadcast operations. [CVE-2015-7973]

The ntpq protocol is vulnerable to replay attacks which may be used to e.g. re-establish an association to malicious server. [CVE-2015-8140]

An attacker who can intercept NTP traffic can easily forge live server responses. [CVE-2015-8139]

Multiple vulnerabilities.

FreeBSD-SA-16:10.linux 27 January 2016

Topic: Linux compatibility layer issetugid(2) system call vulnerability

Category: core
Module: kernel
Announced: 2016-01-27
Credits: Isaac Dunham, Brent Cook, Warner Losh
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-27 07:28:55 UTC (stable/10, 10.2-STABLE)
2016-01-27 07:41:31 UTC (releng/10.2, 10.2-RELEASE-p11)
2016-01-27 07:41:31 UTC (releng/10.1, 10.1-RELEASE-p28)
2016-01-27 07:34:23 UTC (stable/9, 9.3-STABLE)
2016-01-27 07:42:11 UTC (releng/9.3, 9.3-RELEASE-p35)
CVE Name: CVE-2016-1883

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

FreeBSD is binary-compatible with the Linux operating system through a loadable kernel module/optional kernel component. The support is provided on amd64 and i386 machines.

II. Problem Description

A programming error in the Linux compatibility layer could cause the issetugid(2) system call to return incorrect information.

III. Impact

If an application relies on output of the issetugid(2) system call and that information is incorrect, this could lead to a privilege escalation.

issetugid(2) system call vulnerability.

FreeBSD-SA-16:11.openssl 30 January 2016

Topic: OpenSSL SSLv2 ciphersuite downgrade vulnerability

Category: contrib
Module: openssl
Announced: 2016-01-30
Affects: All supported versions of FreeBSD.
Corrected: 2016-01-28 21:42:10 UTC (stable/10, 10.2-STABLE)
2016-01-30 06:12:03 UTC (releng/10.2, 10.2-RELEASE-p12)
2016-01-30 06:12:03 UTC (releng/10.1, 10.1-RELEASE-p29)
2016-01-30 06:09:38 UTC (stable/9, 9.3-STABLE)
2016-01-30 06:12:03 UTC (releng/9.3, 9.3-RELEASE-p36)
CVE Name: CVE-2015-3197

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

FreeBSD includes software from the OpenSSL Project. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

II. Problem Description

A malicious client can negotiate SSLv2 ciphers that have been disabled on the server and complete SSLv2 handshakes even if all SSLv2 ciphers have been disabled, provided that the SSLv2 protocol was not also disabled via SSL_OP_NO_SSLv2.

III. Impact

An active MITM attacker may be able to force a protocol downgrade to SSLv2, which is a flawed protocol and intercept the communication between client and server.

SSLv2 cipher suite downgrade vulnerability.

3.2. Errata Notices

Errata Date Topic

FreeBSD-EN-15:11.toolchain 18 August 2015

Topic: make(1) syntax errors when upgrading from 9.x and earlier

Category: core
Module: toolchain
Announced: 2015-08-18
Credits: John Hein
Affects: FreeBSD 10.2-RELEASE
Corrected: 2015-08-13 22:29:26 UTC (stable/10, 10.2-STABLE)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RC3-p1)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RELEASE-p1)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The FreeBSD userland and kernel build system ensures a seamless upgrade path from the previous major FreeBSD version. During source-based upgrades, the build system must utilize several utilities on the running system in order to bootstrap the build toolchain, after which the bootstrapped utilities are used to produce the build output for the system upgrade.

The make(1) utility was replaced with the NetBSD bmake(1) utility as of FreeBSD 10.0-RELEASE, which has several syntactical differences compared to the fmake(1) utility found in earlier FreeBSD releases.

II. Problem Description

A hard-coded make(1) invocation in the FreeBSD 10.2 sources produce warnings on FreeBSD versions earlier than 10.x due to a syntactical difference between the FreeBSD and NetBSD versions of make(1).

The warnings may persist on FreeBSD 10.2-RELEASE or 10.2-STABLE if the system

is configured to use fmake(1), by defining WITHOUT_BMAKE in src.conf(5).

III. Impact

The warnings produced have no known functional impact. Additionally, the warnings will not recur after the system is upgraded to 10.2-RELEASE or 10.2-STABLE, unless WITHOUT_BMAKE is defined in src.conf(5) as noted above.

Fix make(1) syntax errors when upgrading from FreeBSD 9.x and earlier.

FreeBSD-EN-15:12.netstat 18 August 2015

Topic: Incorrect netstat(1) data handling on 32-bit systems

Category: core
Module: netstat
Announced: 2015-08-18
Credits: Mark Johnston
Affects: FreeBSD 10.2-RELEASE
Corrected: 2015-07-31 00:21:41 UTC (stable/10, 10.2-STABLE)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RC3-p1)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RELEASE-p1)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The netstat(1) utility displays the contents of various network related data structures.

II. Problem Description

The netstat(1) utility incorrectly handles reported values on 32-bit systems.

III. Impact

Due to how netstat(1) processes IPSEC counters, the utility may produce incorrect output on 32-bit systems.

Fix incorrect netstat(1) data handling on 32-bit systems.

FreeBSD-EN-15:13.vidcontrol 18 August 2015

Topic: Allow size argument to vidcontrol(1) for syscons(4)

Category: core

Module: vidcontrol
Announced: 2015-08-18
Credits: Ed Maste
Affects: FreeBSD 10.2-RELEASE
Corrected: 2015-08-04 15:15:06 UTC (stable/10, 10.2-STABLE)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RC3-p1)
2015-08-18 19:30:17 UTC (releng/10.2, 10.2-RELEASE-p1)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The vidcontrol(1) utility is used to set various options for the syscons(4) or vt(4) console driver, such as video mode, colors, cursor shape, screen output map, font, and screen saver timeout.

The vidcontrol(1) utility allows specifying a font size and font file as arguments to the '-f' flag. When no size or file are specified, vidcontrol(1) the default font will be used.

II. Problem Description

The vidcontrol(1) does not properly allow specifying the font size when invoked from the command line.

III. Impact

The vidcontrol(1) utility will use the default font size, regardless of the size specified as an argument to the '-f' flag.
Allow size argument to vidcontrol(1) for syscons(4).

FreeBSD-EN-15:15.pkg 25 August 2015

Topic: Insufficient check of unsupported pkg(7) signature methods

Category: core
Module: pkg
Announced: 2015-08-25
Credits: Fabian Keil
Affects: All supported versions of FreeBSD.
Corrected: 2015-08-19 18:32:36 UTC (stable/10, 10.2-STABLE)
2015-08-25 20:48:51 UTC (releng/10.2, 10.2-RC3-p2)
2015-08-25 20:48:51 UTC (releng/10.2, 10.2-RELEASE-p2)
2015-08-25 20:48:58 UTC (releng/10.1, 10.1-RELEASE-p19)

2015-08-19 18:33:25 UTC (stable/9, 9.3-STABLE)
2015-08-25 20:49:05 UTC (releng/9.3, 9.3-RELEASE-p24)
CVE Name: CVE-2015-5676

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The pkg(8) utility is the package management tool for FreeBSD. The base system includes a pkg(7) bootstrap utility used to install the latest pkg(8) utility.

II. Problem Description

When signature_type specified in pkg.conf(5) is set to an unsupported method, the pkg(7) bootstrap utility would behave as if signature_type is set to "none".

III. Impact

MITM attackers may be able to use this vulnerability and bypass validation, installing their own version of pkg(8).
Insufficient check of supported pkg(7) signature methods.

FreeBSD-EN-15:16.pw 16 September 2015

Topic: Regression in pw(8) when creating numeric users or groups

Category: core
Module: pw
Announced: 2015-09-16
Credits: Thierry Caillet, Baptiste Daroussin
Affects: 10.2-RELEASE
Corrected: 2015-08-23 21:42:27 UTC (stable/10, 10.2-STABLE)
2015-09-16 20:59:41 UTC (releng/10.2, 10.2-RELEASE-p3)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The pw(8) utility is used to create, remove, modify, and display system

users and groups.

II. Problem Description

The pw(8) utility will fail to create users and groups that only contain numeric values [0-9].

III. Impact

An attempt to create a user or group containing only numeric values will fail.

Fix pw(8) regression when creating numeric users or groups.

FreeBSD-EN-15:17.libc 16 September 2015

Topic: libc incorrectly handles signals for multi-threaded processes

Category: core
Module: libc
Announced: 2015-09-16
Credits: Konstantin Belousov
Affects: FreeBSD 10.2
Corrected: 2015-09-05 08:55:51 UTC (stable/10, 10.2-STABLE)
2015-09-16 20:59:41 UTC (releng/10.2, 10.2-RELEASE-p3)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The FreeBSD libc library is the core C runtime library which implements the ANSI C, POSIX APIs and BSD extensions for applications on top of the FreeBSD kernel. The internal operations of libc change when the threading library is loaded, ensuring service implementations are operational in multi-threaded environments, while avoiding unnecessary overhead for applications not utilizing threads. The implementation of some services is delegated to the threading library, for instance, the signal management.

II. Problem Description

Signal-related services, such as signal(3), sigprocmask(2), and sigwait(2) are not properly redirected to the threading library implementation when used by libc directly.

III. Impact

The full impact of the bug is difficult to enumerate precisely based on the nature of the problem, though some visible effects include runtime linker hang during signal delivery, and delivery of a signal to the application at an unexpected time.

Fix libc handling of signals for multi-threaded processes.

FreeBSD-EN-15:18.pkg 16 September 2015

Topic: Implement pubkey support for pkg(7) bootstrap

Category: core
Module: pkg
Announced: 2015-09-16
Credits: Baptiste Daroussin
Affects: All supported versions of FreeBSD.
Corrected: 2015-09-15 05:56:16 UTC (stable/10, 10.2-STABLE)
2015-09-16 20:59:41 UTC (releng/10.2, 10.2-RELEASE-p3)
2015-09-16 21:00:21 UTC (releng/10.1, 10.1-RELEASE-p20)
2015-09-15 08:34:32 UTC (stable/9, 9.3-STABLE)
2015-09-16 21:00:21 UTC (releng/9.3, 9.3-RELEASE-p26)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The pkg(8) utility is the package management tool for FreeBSD. The base system includes a pkg(7) bootstrap utility used to install the latest pkg(8) utility.

II. Problem Description

The pubkey method is not supported by the pkg(7) bootstrap utility. Previously, before EN-15:15.pkg, if the system administrator requested this method, it is silently ignored and no check is performed.

In EN-15:15.pkg, pkg(7) have been modified to issue warning and refuse to proceed any further.

III. Impact

There is no way to use the pubkey method to bootstrap pkg(8) on the system.

Implement pubkey support for pkg(7) bootstrap.

FreeBSD-EN-15:19.kqueue 4 November 2015

Topic: kqueue write events for files greater 2GB would never fire

Category: core
Module: kern
Announced: 2015-11-04
Credits: Steven Hartland
Affects: All supported versions of FreeBSD.
Corrected: 2015-09-24 08:42:08 UTC (stable/10, 10.2-STABLE)
2015-11-04 11:27:13 UTC (releng/10.2, 10.2-RELEASE-p7)
2015-11-04 11:27:21 UTC (releng/10.1, 10.1-RELEASE-p24)
2015-09-24 09:35:35 UTC (stable/9, 9.3-STABLE)
2015-11-04 11:27:30 UTC (releng/9.3, 9.3-RELEASE-p30)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

The kqueue(2) system call provides a generic method of notifying the user when an event happens or a condition holds, based on the results of small pieces of kernel code termed filters.

II. Problem Description

Due to int usage for file offsets in the VOP_WRITE_(PRE|POST) macros, kqueue(2) write events for files greater 2GB were never fired.

III. Impact

Any kqueue(2) consumer monitoring for file changes will fail to receive an event if the monitored file is greater than 2GB.

This causes commands such as 'tail -f' to never see updates.
kqueue(2) write events never fire for files larger than 2GB.

FreeBSD-EN-15:20.vm 4 November 2015

Topic: Applications exiting due to segmentation violation
on a correct memory address

Category: core
Module: kernel
Announced: 2015-11-04

Credits: Konstantin Belousov
Affects: All supported versions of FreeBSD.
Corrected: 2015-09-15 04:20:39 UTC (stable/10, 10.2-STABLE)
2015-11-04 11:27:13 UTC (releng/10.2, 10.2-RELEASE-p7)
2015-11-04 11:27:21 UTC (releng/10.1, 10.1-RELEASE-p24)
2015-10-30 13:05:39 UTC (stable/9, 9.3-STABLE)
2015-11-04 11:27:30 UTC (releng/9.3, 9.3-RELEASE-p30)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The FreeBSD virtual memory system provides processes with virtual address space. Features of virtual address space include copy-on-write pages and page wiring.

II. Problem Description

A race condition exists in the virtual memory implementation. When an application writes to a valid address in its address space, and the corresponding map entry is marked as copy-on-write, and right now undergoes wiring process, and the corresponding page does not yet have a page table entry installed, the application receives a segmentation violation signal. A usual case for this scenario to happen is a write into a never written map entry in a child process right after fork(2) system call.

III. Impact

Under certain conditions, a correctly behaving application could be terminated.
Applications exiting due to segmentation violation on a correct memory address.

FreeBSD-EN-16:01.filemon 14 January 2016

Topic: filemon and bmake meta-mode stability issues

Category: core
Module: filemon
Announced: 2016-01-14
Credits: Bryan Drewery
Affects: FreeBSD 10.2-RELEASE
Corrected: 2015-09-09 17:15:13 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.freebsd.org/>.

I. Background

In FreeBSD 10.2, /usr/bin/make is the NetBSD bmake utility. bmake has a feature called meta-mode [1], which can make use of the filemon(4) kernel module to perform reliable update builds and provide better build dependencies.
[1] http://www.crufty.net/sjg/blog/freebsd-meta-mode.htm

II. Problem Description

Multiple stability and locking problems have been fixed in the filemon(4) kernel module. Without these fixes, using meta-mode and filemon(4) on a FreeBSD 10.2 system may result in kernel panics.

III. Impact

For the jails and virtual machines used by the FreeBSD Jenkins Continuous Integration builders, it is desirable to use released versions FreeBSD. This will allow us to set up builders to test building FreeBSD-CURRENT with meta-mode, using a FreeBSD 10.2-RELEASE-p9 build host.
bmake and filemon(4) stability issues.

FreeBSD-EN-16:02.pf 14 January 2016

Topic: Invalid TCP checksums with pf(4)

Category: core
Module: pf
Announced: 2016-01-14
Credits: Kristof Provost <kp@FreeBSD.org>
Affects: All supported versions of FreeBSD.
Corrected: 2015-11-11 12:36:42 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2015-12-25 15:12:54 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The pf(4) is one of several packet filters available in FreeBSD, originally written for OpenBSD. In addition to filtering packets, it also has packet normalization capabilities.

II. Problem Description

When running with certain network interfaces, capable for hardware transmit checksum offloading, or TCP segmentation offload, pf(4) produces packets with invalid TCP checksums.

III. Impact

The TCP packets with invalid checksums are rejected by the remote host, leading to large performance impacts or inability to successfully run a TCP connection.

Invalid TCP checksum issue.

FreeBSD-EN-16:03.yplib 14 January 2016

Topic: YP/NIS client library critical bug

Category: core
Module: ypclnt
Announced: 2016-01-14
Credits: Ravi Pokala,
Lakshmi Narasimhan Sundararajan,
Fred Lewis,
Pushkar Kothavade
Affects: All supported versions of FreeBSD.
Corrected: 2015-12-21 14:32:29 UTC (stable/10, 10.2-STABLE)
2016-01-14 09:10:46 UTC (releng/10.2, 10.2-RELEASE-p9)
2016-01-14 09:11:16 UTC (releng/10.1, 10.1-RELEASE-p26)
2016-01-13 05:32:24 UTC (stable/9, 9.3-STABLE)
2016-01-14 09:11:26 UTC (releng/9.3, 9.3-RELEASE-p33)

For general information regarding FreeBSD Errata Notices and Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

I. Background

The YP/NIS subsystem allows network management of passwd, group, netgroup, hosts, services, rpc, bootparams and ethers file entries. The ypclnt suite

provides an interface to the YP subsystem.

The standard NIS protocol limits its database entries to YPMAXRECORD (1024 characters).

II. Problem Description

There is a bug with the NIS client library, which can lead to an infinite loop.

III. Impact

A server that is deliberately configured to violate the NIS/YP protocol can cause a FreeBSD NIS client to be stuck forever.
YP/NIS library bug.

4. Userland

This section covers changes and additions to userland applications, contributed software, and system utilities.

4.1. Userland Application Changes

The ar(1) utility now supports a -D flag to prevent real mtime, uid, gid, and file mode values from being inserted. This is called “deterministic mode” and useful for making the resulting archives reproducible. This behavior is enabled by default, and can be disabled by specifying a -U flag.

The camcontrol(8) fwdownload subcommand has been improved. Changes include better support of SATA drives, downloading firmaware to IBM LTO drives, -q flag to suppress information output, and opcodes subcommand to issue the REPORT SUPPORTED OPCODES service action of the SCSI MAINTENANCE IN command.

The cp(1) utility has been updated to include a new flag, -s, which creates a symbolic link to the specified source.

A bug in the ctladm(8) utility which could return a non-zero value even if it succeeds has been fixed.

A bug in the grdc(6) program which caused a wrong display in the 12-hour mode has been fixed.

The ifconfig(8) utility now reports SFP/SFP+ data when a -v flag is specified and the NIC driver provides them.

Bugs in the inetd(8) daemon which could cause a crash when an RPC entry is defined and an IPv6 address is specified in -a flag have been fixed.

The jail(8) utility has been updated to include a new flag, -l, which ensures a clean environment in the target jail when used. Additionally, jail(8) will run a shell within the target jail when run no commands

are specified.

The last(1) utility now supports reboot as a pseudo-user name which prints all system reboot entries (SHUTDOWN_TIME and BOOT_TIME records). This was accidentally removed as of FreeBSD 9.0.

The mv(1) utility now returns 1 instead of 64 when more than two arguments are specified and the target is not a valid directory.

The mkimg(1) utility has been updated to include support for NTFS filesystems in both MBR and GPT partitioning schemes.

A bug in the mkimg(1) utility which prevented dynamic VHD format from working with QEMU has been fixed.

A bug in the netstat(1) utility which showed the statistics in the number of packets divided by 1024, not 1000 has been fixed.

The pciconf(8) utility has been updated to use the PCI ID database from the misc/pciids package, if present, falling back to the PCI ID database in the FreeBSD base system.

A new utility, sesutil(8), has been added, which is used to manage ses(4) devices.

Support for a -manage-gids flag has been added to nfsuserd(8). This option can be enabled at boot time by setting an rc.conf(5) variable nfs_server_managegids to YES.

The pkill(1) utility now supports jail(2) name in a -j option in addition to jail(2) ID.

userdel and usermod subcommand of the pw(8) utility now supports a -y flag.

The resolver library has been updated to reload /etc/resolv.conf if the modification time has changed.

The initial implementation of “reroot” support has been added to the reboot(8) utility, allowing the root filesystem to be mounted from a temporary source filesystem without requiring a full system reboot.

The timeout(1) utility has been added. This utility runs a command with a time limit and is compatible with GNU timeout.

The watchdogd(8) daemon now supports a -x exit_timeout option to specify the timeout period in seconds to leave in effect when the program exits.

The ypinit(8) script now supports eui64 NIS map file.

4.2. Contributed Software

A bug in libarchive(3) library which could report an error when handling a sparse file entry in a tar file has been fixed by importing changeset bf4f6ec64e.

Time zone database has been updated to version 2015f.

The file(1) utility has been updated to version 5.25.

The xz(1) utility has been updated to version 5.2.2, which provides support for multi-threaded compression.

The ntpd(8) utility has been updated to version 4.2.8p5.

The unbound(8) utility has been updated to version 1.5.7.

The less(1) utility has been updated to version v481.

The unbound-control-setup script has been removed from the base system.

The unbound(8) utility has been updated to enable the insecure-lan-zones option in preference of listing each AS112 zone individually.

The OpenSSL suite has been updated to version 1.0.1s.

The OpenSSH suite has been updated to version 7.2p2.

4.3. Installation and Configuration Tools

The bsdinstall(8) utility has been updated to support ZFS installation on EFI-based systems.

4.4. /etc/rc.d Scripts

The rc.d/netwait script has been updated to wait for network interfaces that attach late in the boot process, such as some USB network cards.

Firewall rules set by firewall_type="SIMPLE" now uses ipfw(4) tables for addresses to be blocked.

The rc.d/netif script now updates only static routes when an interface is specified.

5. Kernel

This section covers changes to kernel configurations, system tuning, and system control parameters that are not otherwise categorized.

The vt(4) terminal console driver now supports ALT_BREAK_TO_DEBUGGER and debug.kdb.alt_break_to_debugger sysctl variable when kernel debugger support (options KDB) is enabled.

The vt(4) terminal console driver now supports kern.vt.bell_enable sysctl variable to enable or disable terminal bell. The default is 1 (enabled).

A thread_create() function has been added as an API to create userspace thread in kernel space.

5.1. Kernel Bug Fixes

The kqueue(2) system call has been updated to handle write events to files larger than 2 gigabytes.

5.2. Kernel Configuration

[amd64,i386] The pms(4) driver has been removed from GENERIC kernel.

5.3. System Tuning and Controls

A sysctl(3) variable kern.features.invariants has been added. It shows if the kernel is compiled with INVARIANTS or not.

A bug which could prevent a loader tunable kern.racct.enable from working has been fixed.

6. Devices and Drivers

This section covers changes and additions to devices and device drivers since 10.2-RELEASE.

6.1. Device Drivers

[arm] The imxwdt driver, which supports Freescale i.MX watchdog, has been fixed.

The puc(4) driver now supports MSI interrupts and prefers it to the legacy interrupts. This behavior can be disabled by setting hw.puc.msi_disable loader tunable.

A bug in the uart(4) driver which could cause a polarity reversal of PPS (Pulse Per Second) capture events has been fixed. The trailing edge of a positive PPS pulse and the leading edge of the next pulse were used as "assert" and "clear" event respectively.

The uart(4) driver now supports runtime configuration of PPS signal source captured by the driver via dev.uart.pps_mode and dev.uart.0.pps_mode sysctl variables. The values 0, 1, and 2 correspond to disabled, capturing pulses on the CTS line, and capturing pulses on the DCD line, respectively. The default value is 2.

The uftdi(4) driver now supports UFTDIIOC_READ_EEPROM, UFTDIIOC_WRITE_EEPROM, and UFTDIIOC_ERASE_EEPROM ioctl(2) to read/write serial EEPROM attached to the controller chip.

6.2. Storage Drivers

Legacy ata(4) drivers such as ataahci, ataadaptec, and mv_sata have been removed in favor of the new drivers such as ahci(4), siis(4), and mvs(4).

The CTL High Availability implementation has been rewritten.

The ctl(4) driver has been updated to support CD-ROM and removable devices.

The isp(4) driver has been updated and improved: added support for 16Gbps FC cards, improved target

mode support, completed Multi-ID (NPIV) functionality.

6.3. Network Drivers

The ixgbe(4) driver has been updated to version 3.1.13-k. [r295524] (Sponsored by Limelight Networks, Intel Corporation)

Firmwares for model T4 and T5 bundled with the cxgbe(4) driver have been updated to version 1.14.4.0.

7. Hardware Support

This section covers general hardware support for physical machines, hypervisors, and virtualization environments, as well as hardware changes and updates that do not otherwise fit in other sections of this document.

7.1. Hardware Support

The ismt(4) driver has been added, providing support for recent Intel® SMBus 2.0 controllers.

7.2. Virtualization Support

The xen(4) driver has been updated to include support for blkif indirect segment I/O.

8. Storage

This section covers changes and additions to file systems and other storage subsystems, both local and networked.

8.1. ZFS

The zfs(8) l2arc code has been updated to take ashift into account when gathering buffers to be written to the l2arc device.

9. Boot Loader Changes

This section covers the boot loader, boot menu, and other boot-related changes.

9.1. Boot Loader Changes

Initial terminal emulation support has been added to loader.efi for UEFI-based systems.

Initial ZFS boot support has been added to the EFI implementation.

The UEFI loader has been updated to support multiple ZFS boot environments, such as those provided by sysutils/beadm.

9.2. Boot Menu Changes

The UEFI boot menu has been updated to enable the “Beastie” menu, similiar to the traditional sc(4) boot menu.

10. Networking

This section describes changes that affect networking in FreeBSD.

The epair(4) virtual Ethernet interface and the lagg(4) pseudo interface now support VIMAGE kernel.

A bug in the epair(4) virtual Ethernet interface which could cause a panic when running ifconfig(8) create and destory quickly has been fixed.

sysctl(3) variables in the lagg(4) pseudo interface net.link.lagg.N.* have been removed in favor of per-interface ifconfig(8) flags and options. ifconfig -v command shows them.

Bugs in the lagg(4) pseudo interface which could cause a system panic have been fixed.

A bug in pf(4) packet filter which could cause a rule with no log parameter to log the matched packet has been fixed.

A bug in FreeBSD IPv6 stack which did not invoke an LLENTRY_DELETED event when an L2 address was deleted from the link-level address table for IPv6.

Obsolete APIs, SIOCGDRLST_IN6 and SIOCGPRLST_IN6 in FreeBSD IPv6 stack have been removed.