

Extreme Networks Software

SUMMARY

A possible vulnerability threat has been discovered in the GNU Bash command interpreter and is used by many UNIX and Linux based systems. The vulnerability may allow an attacker to inject commands into a Bash shell, depending on how the shell is invoked. The Bash shell may be invoked by a number of processes including, but not limited to, telnet, SSH, DHCP, and scripts hosted on web servers.

BACKGROUND

GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271. Published: 9/24/2014 9:55:04 PM CVSS Severity: 10.0

The following software, and software supported products by Extreme Networks have been analyzed for this vulnerability:

1. ExtremeXOS
2. Matrix X-Series Secure Core Router
3. N, K, SSA, and S Modular Switches
4. A, B, C, D, & G Series Fixed Switches
5. NetSight / NAC(IA) / Purview
6. Ridgeline
7. IDS/IPS
8. Security Information & Event Manager
9. IdentiFi Wireless
10. Wireless Mobility
11. XSR (X-Pedition Security Router)
12. EWare

IMPACT

The vulnerability impact on Extreme products and technologies identified herein varies depending upon the impacted product and its use configuration and environment.

PRODUCTS POTENTIALLY AFFECTED

These are the software products supported by Extreme Networks that could be affected by this vulnerability:

- NetSight versions 4.x, 5.x, 6.x
- NAC & IA versions 5.0, 5.1, 6.0 and 6.1
- Purview version 6.0 and 6.1
- IDS/IPS versions 7.x, 8.x
- Security Information & Event Manager – All versions
- Wireless Mobility versions WM 5.5.X

Note: To our knowledge, no other Extreme products (including the Enterasys-branded products) have been determined to be vulnerable at this time.

IMPACT DETAILS

The Impact Details will be listed using the following format:

- a. Vulnerable – Yes / No
- b. Vulnerable Component
- c. Conditions when component vulnerability occurs
- d. Product version affected
- e. Workaround
- f. Target Fix Release

ExtremeXOS (all products):

- a. Not Vulnerable (GNU Bash is not used in product)

Matrix X-Series Secure Core Router

- a. Not vulnerable (only admin users have access to GNU Bash)
- b. Bash Shell
- c. Only Admin level users have access to Bash, therefore the vulnerability cannot be exploited by anyone that does not know the admin password. Anybody that knows the admin password can do far more damage directly and does not need to rely on the bash vulnerability.
- d. All X-series products
- e. N/A
- f. N/A

N, K, SSA, and S Modular Switches

- a. Not Vulnerable (GNU Bash is not used in product)

A, B, C, D, & G Series Fixed Switches

- a. Not Vulnerable (GNU Bash is not used in product)

NetSight /NAC (IA)/ Purview:

- a. Yes
- b. SSH Bash shell login
- c. If a non-root user logs into the appliance they can execute commands with elevated access by setting environmental variables in the bash shell
- d. All NetSight /NAC(IA) /Purview appliances (virtual and physical)
 - a. Netsight All versions: 4.x, 5.x, 6.x
 - b. NAC(IA) versions: 5.0, 5.1, 6.0, 6.1
- e. There is no workaround. Customer must install the patch that is now available.
- f. Patch Released for Ubuntu 9/30/14(posted to Extreme Networks download site). Patch for Slackware appliance posted 10/6/14.



IMPACT DETAILS – Cont.

Ridgeline:

- a. No – the OS is not provided with Ridgeline, it is a software application only solution

IDS / IPS:

- a. Yes
- b. SSH Bash shell login
- c. If a non-root user logs into the appliance they can execute commands with elevated access by setting environmental variables in the bash shell.
- d. All appliances
- e. There is no workaround. Customer must install patch that has been posted
- f. Patch released for 8.x Ubuntu appliances 10/2/14 (posted on Extreme Networks download site). Patch for 7.x Slackware appliance posted 10/6/14.

Security Information & Event Manager:

- a. Yes
- b. SSH Bash shell login
- c. If a non-root user logs into the appliance they can execute commands with elevated access by setting environmental variables in the bash shell.
- d. SIEM Appliances at 7.7.0.x, 7.7.1.x, and 7.7.2.x (all versions).
- e. No Workaround
- f. Patch released 10/2/14 (posted on Extreme Networks download site).

Identifi Wireless:

- a. No for Controllers / No for AP's
- b. N/A
- c. 1. APs: Bash is not present in the system
2. Controllers: Bash is present in the system however users cannot get access to it hence the system is not vulnerable to this exploit
- d. N/A
- e. N/A
- f. N/A
- g. N/A

Wireless Mobility:

- a. No for WM3400, 3600, 3700 controllers, No for APs, Yes for WM3951 controller.
- b. WM3951 Controller uses Bash
- c. The WM3951 does have bash shell as part the OS, but access to the bash shell is restricted from all the user interfaces.
- d. WM 5.5.4 and below
- e. No workaround
- f. WM 5.5.5 – Delivery Pending

XSR (X-Pedition Security Router):

- a. Not Vulnerable – Does not use Bash shell.

EWare (all products):

- a. Not Vulnerable – Does not use Bash shell.

Threat Details

CVE	Name	Impact	Vulnerable Versions	Client	Server
CVE-2014-7169	GNU Bash	Critical	Server: GNU Bash through 4.3 bash43-025 Client: GNU Bash through 4.3 bash43-025	Critical	Critical

SYMPTOMS

N/A

WORKAROUND

None



REPAIR RECOMMENDATION

The resolution to any threat or issue is dependent upon a number of things, including the set-up of the computer network and how the local IT team wants to address the situation. Accordingly, in addition to updating the software as recommended in this document, the local IT team will need to analyze and address the situation in a manner that it determines will best address the set-up of its computer network.

Update the software, identified in this Notice, in your Extreme Networks' products by replacing it with the latest releases from Extreme Networks including the following version (or above):

- NetSight / NAC (IA) / Purview: Patch released 9/30/14
- IDS/IPS: Patch released 10/2/14
- Security Information & Event Manager: Patch released 10/2/14
- Wireless Mobility: WM 5.5.4 patch targeted for October

Firmware & Software can be downloaded from - <http://www.extremenetworks.com/support/>

Further Information

NIST release: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271>

Legal Notice

THIS ADVISORY NOTICE IS PROVIDED ON AN "AS IS" BASIS AND EXTREME NETWORKS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESSLY DISCLAIMING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. USE OF THE INFORMATION PROVIDED HEREIN OR MATERIALS LINKED FROM THIS ADVISORY NOTICE IS AT YOUR OWN RISK. EXTREME NETWORKS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME, AND EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE. THE INFORMATION PROVIDED HEREIN IS APPLICABLE TO CURRENT EXTREME NETWORKS' PRODUCTS IDENTIFIED HEREIN AND IS NOT INTENDED TO BE ANY REPRESENTATION OF FUTURE FUNCTIONALITY OR COMPATIBILITY WITH ANY 3RD PARTY TECHNOLOGIES REFERENCED HEREIN. THIS NOTICE SHALL NOT CHANGE ANY CONTRACT OR AGREEMENT THAT YOU HAVE ENTERED INTO WITH EXTREME NETWORKS.

