Silver Peak Security Advisory

GNU Bash Vulnerability, aka “Shellshock”, Published by NIST on 9-24-2014

CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, CVE-2014-7187

Summary:

There is a US-CERT/NIST security advisory originally dated September 24, 2014, for a GNU Bash shell vulnerability, also known as “Shellshock”.

The Shellshock vulnerability exists because of an incomplete fix in a previous Bash vulnerability. As this vulnerability evolved from the initial reports, there are a total of six (6) vulnerabilities in this advisory:

CVE-2014-7169, “Bash: Specially-Crafted Environment Variables Code Injection Attack”

CVE-2014-6271, “Remote Code Execution Through Bash”

CVE-2014-6277, “Bash: Untrusted Pointer Use Issue Leading to Code Execution”

CVE-2014-6278, “Bash: Code Execution Via Specially Crafted Environment Variables”

CVE-2014-7186, “Bash: Parser Can Allow Out-of-Bounds Memory Access While Handling redir_stack”

CVE-2014-7187, “Bash: Off-By-One Error in Deeply Nested Flow Control Constructs”

While Silver Peak products do use affected versions of the Bash shell, Silver Peak appliances do not use CGI scripts, thus an exploit would be extremely difficult since CGI scripts are the most common vector.

SSH is another possible vector, but an exploit using SSH would also be extremely difficult without already having admin login, since the Silver Peak appliance will not allow passing of environment variables from a client.

Only two of the above CVEs describe remote command execution vulnerabilities – these are CVE-2014-7169 and CVE-2014-6271. The other 4 CVEs require login to the bash shell in order to exploit vulnerabilities.

Silver Peak has made available patched versions of Silver Peak VXOA software for download, as well as instructions for patching GMS / GX-V software.

Customers are recommended to upgrade to patched versions of VXOA and to apply the patching instructions for GMS.

The Silver Peak patch referenced throughout this document addresses both remote command execution vulnerabilities (CVE-2014-7169 and CVE-2014-6271) and mitigates both CVE-2014-6277 and CVE-2014-6278 as well.

Later releases will address CVE-2014-7186 and CVE-2014-7187, which are not as critical as they both require a potential attacker to already have logged into a Silver Peak appliance in order to exploit.

Details:

There are 6 advisories related to the Shellshock vulnerability.

The full advisory for CVE-2014-7169 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169, reads as follows:

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.

The full advisory for CVE-2014-6271 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271, reads as follows:

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code 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.

The full advisory for CVE-2014-6277 from NIST, located at https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277, reads as follows:

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access, and untrusted-pointer read and write operations) 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 and CVE-2014-7169.

The full advisory for CVE-2014-6278 from NIST, located at https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278, reads as follows:

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands 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, CVE-2014-7169, and CVE-2014-6277.

The full advisory for CVE-2014-7186 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186, reads as follows:

The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue.

The full advisory for CVE-2014-7187 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187, reads as follows:

Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.

All 6 of these CVEs have been impact rated with CVSS v2 Base Score of 10.0 (HIGH)

For details on NIST impact ratings, browse to:

http://nvd.nist.gov/cvss.cfm?vectorinfo&version=2

Recommended Action for Silver Peak Customers:

Silver Peak has made available patched versions of Silver Peak VXOA software for download, as well as instructions for patching GMS / GX-V software.

Customers are recommended to upgrade to patched versions of VXOA and to apply the patching instructions for GMS.

Silver Peak products use the following versions of GNU Bash:

Silver Peak VXOA:	Bash v3.1.17(1)
Silver Peak GX-V (running Fedora Core 14)	Bash v4.1.7(1)
Silver Peak GX-V (running Fedora Core 12)	Bash v4.0.38(1)

The CVEs listed above are related to the following GNU Bash versions:

* cpe:/a:gnu:bash:1.14.0

* cpe:/a:gnu:bash:1.14.1

* cpe:/a:gnu:bash:1.14.2

* cpe:/a:gnu:bash:1.14.3

* cpe:/a:gnu:bash:1.14.4

* cpe:/a:gnu:bash:1.14.5

* cpe:/a:gnu:bash:1.14.6

* cpe:/a:gnu:bash:1.14.7

* cpe:/a:gnu:bash:2.0

* cpe:/a:gnu:bash:2.01

* cpe:/a:gnu:bash:2.01.1

* cpe:/a:gnu:bash:2.02

* cpe:/a:gnu:bash:2.02.1

* cpe:/a:gnu:bash:2.03

* cpe:/a:gnu:bash:2.04

* cpe:/a:gnu:bash:2.05

* cpe:/a:gnu:bash:2.05:a

* cpe:/a:gnu:bash:2.05:b

* cpe:/a:gnu:bash:3.0

* cpe:/a:gnu:bash:3.0.16

* cpe:/a:gnu:bash:3.1

* cpe:/a:gnu:bash:3.2

* cpe:/a:gnu:bash:3.2.48

* cpe:/a:gnu:bash:4.0

* cpe:/a:gnu:bash:4.0:rc1

* cpe:/a:gnu:bash:4.1

* cpe:/a:gnu:bash:4.2

* cpe:/a:gnu:bash:4.3

Procedure to Patch Silver Peak VXOA hardware or software appliances:

Back up all VXOA appliances and upgrade to ***a patched version of VXOA***. The following builds of VXOA software releases (and any later release) are patched:

VXOA Release 6.2.x:	Build 6.2.5.4_53255
VXOA Release 6.0.x:	Build 6.0.10.1_53298
VXOA Release 5.2.x:	Build 5.2.13.1_53298

Refer to the Silver Peak documentation for details on how to backup and upgrade:

http://www.silver-peak.com/static/UserDocuments/AMOG_R6-2_RevM/wwhelp/wwhimpl/js/html/wwhelp.htm#href=11_System_Mx.13.3.html

Procedure to Patch Silver Peak GMS:

GMS also does not use CGI scripts or pass environment variables so an exploit would be extremely difficult to the best of our knowledge. However, it is recommended to patch the underlying OS (either Fedora Core 12 or Fedora Core 14) using the instructions below:

1. Check the base OS of your GMS server by running the following command in your linux shell:

   ```
   uname –a
   ```

   This should return a value similar to:

   ```
   2.6.35.14-106.fc14.x86_64
   ```

   In this case, there is a string “fc14” within the returned value. This indicates the base OS is Fedora 14. In the case where the base OS is Fedora 12, the returned value will include “fc12”.

2. Get the corresponding RPM file for your base OS (available for download from Silver Peak Support Portal):

   Fedora 14: bash-4.1.7-3.fc14.x86_64.rpm

   Fedora 12: bash-4.0.33-1.fc12.x86_64.rpm

3. Run the following instructions (based on the Fedora Core version determined in Step 1 above):
   a. Fedora 14:
      i. Login as ‘root’ user – contact Silver Peak support for root access
      ii. Copy the rpm file to your /root/ directory.
      iii. Run: rpm –ivh ––force /root/bash-4.1.7-3.fc14.x86_64.rpm
   b. Fedora 12:
      i. Login as ‘root’ user – contact Silver Peak support for root access
      ii. Run: cd /etc/yum.repos.d
      iii. Run: grep -rl '$releasever' ./ | xargs sed -i 's/$releasever/12/g'
      iv. Run: yum install –y rpm

v. Run: yum install –y texinfo
vi. Copy the rpm file to your /root/directory.
vii. Run: rpm –ivh ––force /root/bash-4.0.33-1.fc12.x86_64.rpm

Note for customers running Silver Peak instances in AWS:

The previous version of Silver Peak AMI (VXOA 6.2.2.1) has been updated in the AWS EC2 computing environment with a patched version (VXOA 6.2.5.4).