SHELLSHOCK BASH; MULTIPLE #CVES

PUBLISHED: OCTOBER 01, 2014 | LAST UPDATE: MARCH 13, 2020

SUMMARY

In September 2014, there were additional CVEs spawned from the initial bash CVE-2014-6271 [6], collectively known as Shellshock bash vulnerabilities. These additional CVEs are addressed in this advisory for historic and legacy release families.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2014-6277	CVSS 2.0	10.0 High	bash: specially-crafted environment variables can be used to inject shell commands [1]
2	CVE-2014-6278	CVSS 2.0	10.0 High	bash: incorrect parsing of function definitions with nested command substitutions [2]
3	CVE-2014-7169	CVSS 2.0	10.0 High	bash: code execution via specially-crafted environment (Incomplete fix for CVE-2014-6271) [3]
4	CVE-2014-7186	CVSS 2.0	10.0 High	bash: parser can allow out-of-bounds memory access while handling redir_stack [4]
5	CVE-2014-7187	CVSS 2.0	10.0 High	bash: off-by-one error in deeply nested flow control constructs [5]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
2.6.1-GR1	–	2.6.1-GR1-Px	2.7.2-P16, 4.1.0, 4.1.1, 4.1.4-GR1, 5.1.0
2.6.6-GR1	–	2.6.6-GR1-Px	2.8.2-P11, 4.1.2, 4.1.4-GR1, 5.1.0
2.7.0	–	2.7.0-Px	2.7.2-P16, 4.1.0, 4.1.1, 4.1.4-GR1, 5.1.0
2.7.1	–	2.7.1-Px	2.7.2-P16, 4.1.0, 4.1.1, 4.1.4-GR1, 5.1.0
2.7.2	–	2.7.2-P15	2.7.2-P16, 4.1.0, 4.1.1, 4.1.4-GR1, 5.1.0
2.8.0	–	2.8.0-Px	2.8.2-P11, 4.1.2, 4.1.4-GR1, 5.1.0
2.8.1	–	2.8.1-P2	2.8.2-P11, 4.1.2, 4.1.4-GR1, 5.1.0
2.8.2	–	2.8.2-P10	2.8.2-P11, 4.1.2, 4.1.4-GR1, 5.1.0
2.9.1	–	3.2.1-Px (TPS)	3.2.2-P1
2.5.0	–	2.6.0 (aGalaxy)	3.0.1, 3.2.2, 5.0.0 (aGalaxy)

WORKAROUNDS AND MITIGATIONS

See the workarounds and mitigations for the affected release described in the security advisory “A10 Vulnerability to "Shellshock Bash" #CVE-2014-6271” [7].

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2014-6277	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.
CVE-2014-6278	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.
CVE-2014-7169	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.
CVE-2014-7186	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.
CVE-2014-7187	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.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2014-6277
[2]	NIST NVD, CVE-2014-6278
[3]	NIST NVD, CVE-2014-7169
[4]	NIST NVD, CVE-2014-7186
[5]	NIST NVD, CVE-2014-7187
[6]	NIST NVD, CVE-2014-6271
[7]	A10 Security Advisory - A10 Vulnerability to "Shellshock Bash" #CVE-2014-6271

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2014-10-01	Initial Publication
1.1	2018-04-16	Created web page
2.0	2020-02-17	Refactored advisory for contemporary structure and format. Added affected releases, workaround, vulnerability details, and related links content.
2.1	2020-03-13	Adjust aGalaxy fix versions