SSH - CVE-2016-3115, CVE-2010-5107

PUBLISHED: AUGUST 8, 2017 | LAST UPDATE: AUGUST 8, 2017

SUMMARY

Vulnerability scans of the ACOS management interface indicate potential security exposures in the SSH, remote access service. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	QID: 38623	Qualys	3 Serious	OpenSSH Xauth Command Injection Vulnerability
2	CVE-2016-3115	CVSS 3.0	6.4 Medium	Multiple CRLF injection vulnerabilities in session.c [1]
3	QID: 42413	Qualys	3 Serious	OpenSSH LoginGraceTime Denial of Service Vulnerability
4	CVE-2010-5107	CVSS 2.0	5.0 Medium	openssh: Prevent connection slot exhaustion attacks [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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
			4.1.2 [(a)]
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.0	–	4.1.0-P8	4.1.0-P9
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
2.8.2	–	2.8.2-P8	4.1.2
2.7.2	–	2.7.2-P7	4.1.0-P9, 4.1.1-P3
2.7.1	–	2.7.1-GR1-P1	4.1.0-P9, 4.1.1-P3
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P9, 4.1.1-P3

[(a)] Including all updates to the release(s).

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

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
QID: 38628	OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol. The sshd server fails to validate user-supplied X11 authentication credentials when establishing an X11 forwarding session. An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. Please note that Systems with X11Forwarding enabled are affected. Reference: CVE-2016-3115.
CVE-2016-3115	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.
QID: 42413	OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol. Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion. Reference: CVE-2010-5107.
CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2016-3115
[2]	NIST NVD, CVE-2010-5107

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-08	Initial Publication