SSH - CVE-2015-5600

PUBLISHED: JULY 28, 2017 | LAST UPDATE: JULY 28, 2017

SUMMARY

A vulnerability in OpenSSH has been identified that could allow attackers conducting brute force attacks to bypass security restrictions or cause Denial of Service (DoS) on targeted systems. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2015-5600	CVSS 2.0	8.5 High	Large # KBD devices can bypass MaxAuthTries [1]

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-P3	2.8.2-P4
2.7.2	–	2.7.2-P7-SP2	2.7.2-P7-SP3, 2.7.2-P8
2.7.1-GR1	–	2.7.1-GR1	2.7.1-GR1-P1
2.7.0	–	2.7.0-P7	2.7.0-P8
2.6.1-GR1	–	2.6.1-GR1-P15	2.6.1-GR1-P16

[(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
CVE-2015-5600	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2015-5600

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-07-28	Initial Publication