RAPID RESPONSE
Security Advisory

SECURITY ADVISORY

#CVE-2015-5621 published on September 1st, 2015

Summary Description

This security advisory addresses CVE-2015-5621, pertaining to a bug in the net-snmp software affecting versions up to and including 5.7.2. This vulnerability allows for potential denial of service and hypothetically can lead to remote code execution.

Details

Some version of ACOS, include vulnerable version of the net-snmp libraries, and can potentially be affected by this vulnerability. The effect is known to be able to cause crash in the SNMP process which will lead to unavailability of that component, while the rest of the functionality, including the data plane will not be affected.

Furthermore, some publications indicate that a remote execution of code is theoretically possible.

The A10 QA team has not been able to cause either of those outcomes however patches are being proactively released due to the potential severity of the issue.

Mitigation Recommendations

In regular deployments SNMP is only exposed on the management interface which already limits the exposure significantly. In addition to that it is recommended that access is further limited through Access Control Lists (ACLs) to only select IP management IP addresses. In addition to that, it is recommended that perimeter ACLs ensure no management IP addresses can be spoofed from outside the relevant network segments.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.0.1, 3.1.x, 2.7.2-P5, 2.7.1-GR1, 2.8.2-P3*

Software Updates

Software updates resolving this potential vulnerability will be published at the following URL when available:

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

The following table summarizes update versions resolving all of the above CVEs.

Vulnerable Release	Resolved Release
4.0.1	4.1.0
3.0.x	3.2.0
3.1.x	3.2.0
2.6.1-GR1-P15	2.6.1-GR1-P16
2.7.2-P5	2.7.2-P6
2.7.1-GR1	2.7.1-GR1-P1
2.8.2-P3	2.8.2-P4

References

1. OpenSSL Security Advisory – 2015-03-08: https://www.openssl.org/news/secadv_20150611.txt
2. NIST-NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5621
3. MITRE-DB, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5621