SECURITY ADVISORY

#CVE-2015-0235 published on January 28th, 2015

UPDATED February 2nd, 2015, with these changes: In summary of updates table 2.6.1-GR1-P15 replaced with 2.6.1-GR1-P14-SP1.
UPDATED February 10th, 2015, with these changes: Updated first paragraph of section "Details as Pertaining to A10 Software and Equipment."

Summary Description

On January 27th, 2015, buffer overflow vulnerability in glibc affecting versions 2.2 to 2.17 was released by Qualys. It affects the __nss_hostname_digits_dots() and can be triggered in a few different ways, all of which require the attacker to have a certain control over the arguments passed to the function. In their advisory, Qualys calls in particular the legacy functions gethostbyname*().

The vulnerability is assigned CVE-2015-0235 (see References below).

Details as Pertaining to A10 Software and Equipment

A10 analyzed all calls to the deprecated gethostbyname*() functions, as well as the underlying culprit __nss_hostname_digits_dots(), in our codebase. It appears the use of those functions is very limited and only constrained to components reading user-supplied configuration files/options; thus, in the unlikely event of successful exploitation, a user, who already has administrative privileges, may be able to crash the configuration process or execute arbitrary code. Since the user would require administrative access to do that, no privilege escalation could occur and crashing the system would be equivalent to that system user issuing the shutdown command.

Nevertheless, engineering is already in the process of upgrading the software to include unaffected versions of the glibc library. The patches in which this will be fixed are summarized in the "Software Updates" section. For timelines, please refer to the A10 support web site.

Also, if we discover any risks for particular software trains, we will issue special patches.

In addition to core OS code, A10 appliances offer the ability to execute custom health check scripts. It is possible that those health checks invoke some of the legacy functions with data supplied of less trusted entity. We cannot assess this scenario since we do not have access to, nor support, those customer-created custom scripts—but we want to warn customers to investigate this potential issue.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS, HVA, a Galaxy*

Affected Software Versions: *2.6.1-GR1-X, 2.7.X, 2.6.6-GR1-x, 2.8.x, TPS 2.9.1, TPS 3.x.x.*

Mitigation Recommendations

Since the only possible way to pass user-controlled data to the device is through the configuration mechanism, it is recommended that customers evaluate if some automated processes are allowing untrusted data (namely IP addresses) to be included in the configuration files.

In the case of custom health check scripts, the customer needs to do an assessment and decide the best way to mitigate if necessary.

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#CVE-2015-0235

The following table summarizes update versions.

Vulnerable Release	Resolved Release
3.0.0-TPS-P2-SP17	3.0.0-TPS-P2-SP18
3.1.0-SP1	3.1.1
3.1.0-P1	3.1.1
2.9.1-P2-SP26	3.0.0-TPS-P2-SP18
2.6.1-GR1-P14	2.6.1-GR1-P14-SP1
2.7.0-P6	2.7.0-P7
2.7.1-P6	2.7.1-GR1
2.7.2-P4	2.7.2-P5
2.6.6-GR1-P5	2.6.6-GR1-P6
2.8.0-P4	2.8.0-P5
2.8.1-P2	2.8.1-P3
2.8.2-P2	2.8.2-P3
4.0.0	4.0.1

References

1. Qualys Security Advisory CVE-2015-0235, https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt
2. MITRE CVE Database, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235