SECURITY ADVISORY

#CVE-2015-7547 published on February 18th, 2016

Summary Description

This security advisory addresses CVE-2015-7547, pertaining to the GNU C Library vulnerability triggered when the getaddrinfo function is called.

Details

In cases where glibc expects data larger than 2048 bytes of data, it allocates additional buffer in the heap and after the stack based buffer is full it continues to copy the date to the heap. It was discovered that in some cases glibc fails to properly handle the incoming data and writes it on the stack instead of the allocated heap buffer. More details can be found in the references 1-4.

When performing DNS resolution it is possible for an attacker to craft a response that would trigger the vulnerability and either cause a crash of the process or execute arbitrary code on the system.

In order to successfully exploit, the attacker must be in control of a domain and DNS server that the device will directly talk to, which severely limits the attack vectors.

In addition it is possible to execute this attack if the attacker can man-in-the-middle or can beat the legitimate server in providing the answer, which again implies access to network resources and position which is non-trivial to achieve.

In the POC published the SSH process is implicated, however this is not limited to it. This vulnerability can be triggered by a large number of processes that use the getaddrinfo function.

Overall the exploitation of the vulnerability is very difficult to achieve but if successful, the impact can be very high. This is why we rank this vulnerability as high severity.

Mitigation

Since the essence of the vulnerability is failure to properly sanitize input, one of the solutions is to ensure all answers to the affected system are coming from trusted sources over a medium (network) that is relatively secure.

The best way to mitigate the risk from this vulnerability is to only allow the appliance to use local recursive resolvers that would sanitize the responses going to it.

There are some less practical mitigation, that may not be possible in all cases. Those would be:

- drop dual A/AAAA queries going to a network segment with affected devices;
- drop UDP packets larger than 512 (breaks EDNS0)
- limit TCP responses to 2048 bytes

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.x, 3.x*

Software Updates

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

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

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

Vulnerable Release	Resolved Release
4.x	4.1.0
3.x	3.2.1

References

1. NIST-NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7547
2. MITRE-DB, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547
3. RedHat, https://access.redhat.com/security/cve/cve-2015-7547
4. Google BlogPost, https://googleonlinesecurity.blogspot.ca/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html?m=1