VASCO Security Advisory

CVE-2015-7547 vulnerability in VASCO products

Advisory ID: vasco-sa-20160223-glibc

Revision number: 1.0

Date and time of release: February 23 2016 12:00 UTC

Date and time of last update: February 23 2016 12:00 UTC

Summary

On Tuesday February 16, 2016 Google engineers published a blog post on a vulnerability found in all versions of glibc since 2.9. The blog post explaines that the glibc DNS client side resolver is vulnerable to a stack-based buffer overflow when the getaddrinfo() library function is used. Software using this function may be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack.

Impacted products

Following products are affected by the CVE-2015-7547 vulnerability:

- IDENTIKEY Federation Server 1.6
- IDENTIKEY Appliance 3.4.5.0 and later
- AXSGUARD Gatekeeper 7.7.0 and later

Even though the vulnerable version of glibc is used in these products, VASCO rates the exploitability low because of the way the DNS client side resolver is being used in the products.

Detailed description of vulnerability

The following vulnerability description is extracted from the NIST National Vulnerability Database:

“Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.”

Severity score

The table below denotes the CVSS 2.0 vulnerability score of vulnerability CVE-2015-7547.

CVSS Base Score: 6.8 (medium)					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	Partial	Partial	Partial

Product fixes and workarounds

VASCO will fix vulnerability CVE-2015-7547 in the following upcoming releases:

- IDENTIKEY Federation Server 1.6.1 (to be released in the first quarter of 2016)
- IDENTIKEY (Virtual) Appliance 3.10.11.0 (to be released in the second quarter of 2016)
- AXSGUARD GateKeeper 8.2.1 (to be released in the second quarter of 2016)

VASCO recommends customers using IDENTIKEY Authentication Server to update the glibc library using the update system of their distribution.

Obtaining product releases with fixes

For aXsGUARD Gatekeeper products:

- VASCO will deploy patches via the automated update service. Customers that do not allow their system to receive updates via this service should contact VASCO for instructions about how to obtain the patch.

For other products:

- Customers with a maintenance contract can obtain fixed product releases from MyMaintenance. Customers without a maintenance contract should contact their local sales representative.

References

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7547
- https://googleonlinesecurity.blogspot.be/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html

Legal disclaimer