VASCO Security Advisory

glibc GHOST vulnerability in VASCO products

Advisory ID: vasco-sa-20150202-ghost

Revision number: 1.0

Date and time of release: February 04 2015 12:00 UTC+1

Date and time of last update: February 04 2015 12:00 UTC+1

Summary

On January 27, 2015, security researchers from Qualys publicly announced a vulnerability in the GNU C library, known as glibc. The vulnerability, which is commonly referred to as GHOST, may allow an unauthenticated, local or remote attacker to take control of systems. The first vulnerable version of the GNU C Library is glibc-2.2, released on November 10, 2000.

Impacted products

Following products are affected by the GHOST vulnerability:

- IDENTIKEY Federation Server 1.4, 1.5
- IDENTIKEY Appliance (all versions)
- aXsGUARD Gatekeeper (all versions)

Detailed description of vulnerability

The GNU C library glibc is the implementation of the standard library of the C programming language by the GNU Project. The C standard library provides basic functions for interaction with operating system services, input/output processing, memory allocation, and other types of functions.

The GNU C library contains a function named __nss_hostname_digits_dots(), which is used by the gethostbyname() and gethostbyname2()functions. The two latter functions allow applications to resolve DNS queries.

The function __nss_hostname_digits_dots() contains a heap-based buffer overflow. A local or remote attacker can use this vulnerability to execute arbitrary code with the permissions of the user running the application.

However, the functions gethostbyname() and gethostbyname2() have been deprecated for approximately fifteen years, mainly because of lack of support of IPv6.

The vulnerability is commonly referred to as GHOST, and has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2015-0235.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of this vulnerability.

CVSS Base Score: 10.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score: 7.8					
Exploitability		**Remediation Level**		**Report Confidence**	
Proof-of-Concept		Official Fix		Confirmed	

Product fixes and workarounds

VASCO will release following patches:

- IDENTIKEY Federation Server 1.4.5 and 1.5.4 on February 6th 2015
- IDENTIKEY Appliance 3.8.9.0 in April 2015
- For aXsGUARD Gatekeeper 8.1.0: Hotfix 001 on February 6th 2015

VASCO recommends customers using IDENTIKEY Authentication Server 3.4 SR1 and 3.5 to upgrade to version 3.6. VASCO recommends customers using IDENTIKEY Authentication Server 3.6 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 updated 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235

Legal disclaimer

THE INFORMATION IN THIS DOCUMENT AT ANY TIME AND AT ITS DISCRETION, AS AND WHEN NEW OR ADDITIONAL INFORMATION BECOMES AVAILABLE.