VASCO Security Advisory

GNU Bash Environment Variable Command Injection Vulnerability in VASCO products

Advisory ID: vasco-sa-20140930-bash

Revision number: 1.0

Date and time of release: September 30 2014 12:00 UTC+1

Date and time of last update: October 17 2014 12:00 UTC+1

Summary

On September 24, 2014, the GNU foundation publicly announced a vulnerability in the GNU Bash shell. Bash is a Unix shell developed as part of the GNU project as a replacement for the Bourne shell (sh). It has been distributed widely as part of the GNU operating system and is the default shell for Linux and OS X. The vulnerability is commonly referred to as the "shellshock" vulnerability.

Many Internet daemons, including telnet, SSH and web servers, invoke the Bash shell. The Bash shell uses environment variables to pass information into processes that are spawned from it. The vulnerability allows an attacker to inject arbitrary commands into a Bash shell using specially crafted environment variables.

The specific impact of the vulnerability depends on the process using the Bash shell. In the worst case, an unauthenticated remote attacker would be able to execute commands on an affected server.

Impacted products

Following VASCO products and services are affected by the vulnerability:

- aXsGUARD Gatekeeper (all versions)
- IDENTIKEY Federation Server (versions 1.3, 1.4 and 1.5)
- MYDIGIPASS.COM

Detailed description of vulnerability

The Bash shell uses environment variables to pass information into processes that are spawned from it. Environment variables can be used to store function definitions. Such environment variables start with "() {" and usually end with "};".

However Bash executes any code in the environment variable after the function definition. This allows an attacker to create a function definition such as:

```
FUNCT=() { ignore; }; echo shellshock
```

This would cause the code "echo shellshock" to be executed when Bash processes its environment variables.

The impact of this vulnerability on VASCO products varies depending on the affected product and the nature of the product usage.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) IDs CVE-2014-6271 and CVE-2014-7169.

Severity score

The tables below denote the CVSS 2.0 vulnerability score.

1) Attack vectors that do not require authentication

CVSS Base Score: 7.5					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score: 7.1					
Exploitability		**Remediation Level**		**Report Confidence**	
Functional		Not defined		Confirmed	

2) Attack vectors that require authentication

CVSS Base Score: 6.5					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	Single	Partial	Partial	Partial
CVSS Temporal Score: 6.2					
Exploitability		**Remediation Level**		**Report Confidence**	
Functional		Not defined		Confirmed	

Product fixes and workarounds

VASCO has patched following products:

- aXsGUARD Gatekeeper 7.6.5, 7.7.0, 7.7.1, 7.7.2 and 7.7.3

VASCO has patched following service:

- MYDIGIPASS.COM

VASCO will release patches for following products:

- IDENTIKEY Federation Server 1.4.4 and 1.5.3, to be released on October 22, 2014

Obtaining product releases with fixes

- For aXsGUARD Gatekeeper products:

  VASCO has already deployed patches for aXsGUARD Gatekeeper products 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 sales representative.

References

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

Legal disclaimer

WHILE EVERY REASONABLE EFFORT IS MADE TO PROCESS AND PROVIDE INFORMATION THAT IS ACCURATE, ALL THE CONTENT AND INFORMATION IN THIS DOCUMENT ARE PROVIDED "AS IS" AND "AS AVAILABLE," WITHOUT ANY REPRESENTATION OR ENDORSEMENT AND WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OF CURRENCY, COMPLETENESS OR SUITABILITY, OR ANY WARRANTY INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE. YOUR USE OF THIS DOCUMENT, ANY INFORMATION PROVIDED, OR OF MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. VASCO RESERVES THE RIGHT TO CHANGE OR UPDATE THE INFORMATION IN THIS DOCUMENT AT ANY TIME AND AT ITS DISCRETION, AS AND WHEN NEW OR ADDITIONAL INFORMATION BECOMES AVAILABLE.