VASCO Security Advisory

SSL 3.0 POODLE vulnerability in VASCO products

Advisory ID: vasco-sa-20141017-poodle

Revision number: 1.0

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

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

Summary

On October 14 2014 security researchers from Google publicly announced a vulnerability in version 3.0 of the Secure Sockets Layer (SSL) protocol. The vulnerability allows an unauthenticated, remote attacker to decrypt portions of communications that are encrypted using the Cipher Block Chaining (CBC) mode of operation for block ciphers. The vulnerability is commonly referred to as Padding Oracle On Downgraded Legacy Encryption (POODLE).

Impacted products

Following products are affected by the POODLE vulnerability:

- IDENTIKEY Server 3.3, 3.4
- IDENTIKEY Authentication Server 3.4 SR1, 3.5
- IDENTIKEY Federation Server 1.3, 1.4, 1.5
- IDENTIKEY Appliance 3.2.4.{2,3}, 3.4.5.{0,1}, 3.4.6.{0,1}
- IDENTIKEY Virtual Appliance 3.4.6.{0,1}
- aXsGUARD Gatekeeper (all versions)

Detailed description of vulnerability

Secure Sockets Layer (SSL) 3.0 is a cryptographic protocol used to protect the confidentiality and integrity of data exchanged over IPv4 and IPv6 networks. On October 14 2014 security researchers from Google publicly announced a vulnerability in the SSL 3.0 protocol. The vulnerability allows an unauthenticated, remote attacker who acts as a man-in-the-middle to decrypt portions of communications that are encrypted using the Cipher Block Chaining (CBC) mode of operation for block ciphers. More specifically the vulnerability allows the attacker to decrypt a certain byte of ciphertext with at most 256 attempts. The vulnerability exists because of the sequence of encryption and message authentication, and because of the type of padding in SSL 3.0.

The vulnerability is commonly referred to as Padding Oracle On Downgraded Legacy Encryption (POODLE). It does not apply to Transport Layer Security (TLS) protocols.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2014-3566.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of the various vulnerabilities.

CVSS Base Score: 2.6					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	High	None	Partial	None	None

CVSS Temporal Score: 2.5		
Exploitability	**Remediation Level**	**Report Confidence**
Functional	Unavailable	Confirmed

Product fixes and workarounds

VASCO will release following patches:

- IDENTIKEY Federation Server 1.4.4, 1.5.3 on October 22 2014

VASCO will release following products:

- aXsGUARD Gatekeeper 8.0.0, as from October 23 2014

Customers using IDENTIKEY Federation Server 1.3 are recommended to upgrade IDENTIKEY Federation Server 1.4 or 1.5 and apply the corresponding patch.

Customers using impacted versions of IDENTIKEY Server or IDENTIKEY Authentication Server are recommended to upgrade to IDENTIKEY Authentication Server 3.6, in which SSL 3.0 is disabled by default. Alternatively customers can manually disable SSL 3.0 and enable TLS 1.x.

Customers using impacted versions of IDENTIKEY Appliance or IDENTIKEY Virtual Appliance are recommended to upgrade to IDENTIKEY (Virtual) Appliance 3.4.6.2 or higher, in which SSL 3.0 is disabled by default.

Customers using impacted versions of aXsGUARD Gatekeeper can manually disable SSL 3.0 or upgrade to version 8.0.0, in which SSL 3.0 is disabled by default.

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

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- https://www.openssl.org/~bodo/ssl-poodle.pdf

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.