COMODO

Creating Trust Online®

Comodo CA

Advisory and Response to 'Heartbleed' OpenSSL Vulnerability

04/08/2014

Table of Contents

Overview

- All customers are advised to patch systems to run the latest version of OpenSSL
- Vulnerability lies with OpenSSL, not with Comodo certificates or Comodo CA keys
- Certificates on affected systems need to be replaced, free of charge, with immediate effect
- Customers can order a certificate reissue via our web-interface, management portal or the APIs. Contact **support@comodo.com** if help is required.

In the light of the recently discovered vulnerability known as 'Heartbleed', Comodo CA, a leading Certificate Authority and Internet security organization, would like to confirm that the vulnerability lies with the OpenSSL software and not with Comodo certificates or Comodo CA keys. Comodo will work with customers, partners, platform vendors and service providers to help ensure affected parties are made fully aware of the issue over the coming days, that customers systems are updated with the fixed version of OpenSSL with immediate effect, and that customers can quickly and easily acquire a certificate re-issuance that may be required as a result of patching OpenSSL.

What is the 'Heartbleed' Vulnerability?

On Tuesday 7th of April 2014, a serious vulnerability to OpenSSL known as 'Heartbleed' was made public by a team of researchers.

The 'Heartbleed' vulnerability means that it is possible for an attacker to silently 'steal' private keys for SSL certificates, as well as other secret information, on affected versions of OpenSSL.

OpenSSL is an incredibly popular cryptographic software library, and provides SSL/TLS communication for large numbers of applications. The bug causing the vulnerability was introduced to OpenSSL in December 2011 and has been 'in the wild' since the release of OpenSSL 1.0.1 on 14th March 2012. However, it was only discovered within the past day and, other than a proof of concept, Comodo is not aware of any real-world exploits at this point in time.

Full details of the vulnerability, including more technical details, can be found at: **http://heartbleed.com/**

What is affected?

OpenSSL versions affected: 1.0.1 through to 1.0.1f (inclusive).

The following OpenSSL versions are NOT affected:

1.0.1g

1.0.0 (entire branch)

0.9.8 (entire branch)

The release of OpenSSL 1.0.1g on the 7th April 2014 fixes the bug.

How do I fix it?

Any systems using vulnerable versions of OpenSSL need to be patched or updated.

OpenSSL themselves have released a patch, and many other software vendors have updated their software as well.

Please contact your vendor for further details.

Patch your server **before** you install your new certificate. If you put a new certificate onto a vulnerable server you risk compromising the key of the new certificate.

Is my site affected?

Customers can test whether they are affected by visiting **https://sslanalyzer.comodoca.com/** to verify the presence of this vulnerability.

What about my certificates?

Because there is a theoretical possibility that Heartbleed could already have been exploited, Comodo must replace certificates on systems running the affected OpenSSL version. Certificates on affected systems should be replaced, as soon as possible and the previous certificates should be revoked.

Comodo have ensured that all of our own websites using OpenSSL have been patched and updated, and we have also reissued certificates for those sites as a precautionary measure. We know it is a big task that you did not ask for, but like any other web-server vulnerability it requires your urgent attention.

Comodo, unlike other CAs, has a no-charge reissue policy - so replacing your certificate and maintaining the security of your website and your systems is simple and incurs no additional cost.

To perform a reissue, please follow the normal procedures - reissuing via our web-interface, management portal or the APIs **https://support.comodo.com/**

References:

http://heartbleed.com/

https://www.openssl.org/news/secadv_20140407.txt

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

STE 100

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com**.