



COT Security Alert – OpenSSL Heartbleed Vulnerability

A vulnerability in versions of OpenSSL 1.0.1 before 1.0.1g has been reported to the Chief Information Security Office by US-CERT (United States Computer Emergency Readiness Team) and other trusted sources. The vulnerability could result in information disclosure from affected secure sites. Affected sites could allow an attacker access to sensitive data, including private keys, logon credentials and confidential data in the server memory.

COT has applied defensive rules on network security devices which are designed to monitor and, where possible, block these attacks. In addition web assets have been patched as they were found vulnerable. Despite these efforts, full remediation on an affected server may require generating new public-private key pairs and revoking and reissuing SSL certificates as it is not possible to know if they have already been compromised.

Users should change passwords after these security measures have been taken.

Recommendations:

1. Security patches should be applied promptly after testing.
2. Affected sites should revoke and replace their current SSL certificate.
3. Users should change online passwords once an affected server is secured.

For more information, review the online sources provided below.

<http://www.us-cert.gov/ncas/current-activity/2014/04/08/OpenSSL-Heartbleed-Vulnerability>

<http://www.kb.cert.org/vuls/id/720951>

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Service Desk at 502.564.7576.

Office of Chief Information Security Officer
Commonwealth Office of Technology
Frankfort, KY 40601
technology.ky.gov

Technology-enabled Business Solutions for 21st Century Government