Title Security Bulletin: IBM SDN for Virtual Environments is affected by a vulnerability in OpenSSL (CVE-2014-0160)

Summary A security vulnerability has been discovered in OpenSSL.

Vulnerability Details

CVE-ID: CVE-2014-0160

DESCRIPTION: OpenSSL could allow a remote attacker to obtain sensitive information, caused by an error in the TLS/DTLS heartbeat functionality. An attacker could exploit this vulnerability to expose 64k of private memory and retrieve secret keys. An attacker can repeatedly expose additional 64k chunks of memory. This vulnerability can be remotely exploited, authentication is not required and the exploit is not complex. It can be exploited on any system (ie. server, client, agent) receiving connections using the vulnerable OpenSSL library.

CVSS Base Score: 5
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/92322
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Warning: We strongly encourage you to take action as soon as possible as potential implications to your environment may be more serious than indicated by the CVSS score.

Affected Products and Versions

IBM SDN VE, Unified Controller, VMware Edition: 1.0.0
IBM SDN VE, Unified Controller, KVM Edition: 1.0.0
IBM SDN VE, Unified Controller, OpenFlow Edition: 1.0.0
IBM SDN VE, Dove Management Console, VMware Edition: 1.0.0

Remediation/Fixes

IBM recommends updating affected IBM SDN VE, Unified Controllers to the latest versions of IBM SDN VE for which IBM is providing a fix, which are identified below:

IBM SDN VE, Unified Controller, VMware Edition: version 1.0.1 or later
IBM SDN VE, Unified Controller, KVM Edition: version 1.0.1 or later
IBM SDN VE, Unified Controller, OpenFlow Edition: version 1.0.1 or later

These versions are available via Passport Advantage.

After applying the fix, additional instructions are needed for CVE-2014-0160

1) Replace your SSL Certificates.

> You need to revoke existing SSL certificates and reissue new certificates. You need to be sure not to generate the new certificates using the old private key and create a new private key (ie using "openssl genrsa") and use that new private key to create the new certificate signing request (CSR).

2) Reset User Credentials

> Users of network facing applications protected by a vulnerable version of OpenSSL should be forced to reset their passwords and should revoke any authentication or session related cookies set prior to the time OpenSSL was upgraded and force the user to re-authenticate.

Warning: Your environment may require additional fixes for other products, including non-IBM products. Please replace the SSL certificates and reset the user credentials after applying the necessary fixes to your environment.

Workarounds and Mitigations

None known

Reference

- *Complete CVSS Guide*
- *On-line Calculator V2*
- *OpenSSL Project vulnerability website*
- *Heartbleed*

Related Information

IBM Secure Engineering Web Portal
IBM Product Security Incident Response Blog

Acknowledgement

None

Change History

16 April 2014: Original Copy Published

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.