Title Security Bulletin: IBM SDN for Virtual Environments is affected by a vulnerability in OpenSSL (CVE-2014-0224)

Summary A security vulnerability has been discovered in OpenSSL.

Vulnerability Details

CVE-ID: CVE-2014-0224

DESCRIPTION: An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server. The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1. Users of OpenSSL servers earlier than 1.0.1 are advised to upgrade as a precaution.

CVSS Base Score: 5.8
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/93586 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:N)

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
IBM SDN VE, Unified Controller, VMware Edition: 1.0.1
IBM SDN VE, Unified Controller, KVM Edition: 1.0.1
IBM SDN VE, Unified Controller, OpenFlow Edition: 1.0.1
IBM SDN VE, Dove Management Console, VMware Edition: 1.0.1

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 1.0.2 or later
IBM SDN VE, Unified Controller, KVM Edition: version 1.0.2 or later
IBM SDN VE, Unified Controller, OpenFlow Edition: version 1.0.2 or later
These versions are available via Passport Advantage.

Workarounds and Mitigations

None known

Reference

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

Related Information

IBM Secure Engineering Web Portal
IBM Product Security Incident Response Blog

Acknowledgement

None

Change History

18 July 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.