Advisory Alert

Alert No: AAA171212 Date: 12-Dec-17 10:54 AM

Security Updates for 12th December 2017

Overview		
High	Microsoft	▪ Remote Code Execution
Medium and Low	OpenSSL	▪ Bypass Security Restrictions
	IBM WebSphere	▪ Denial of Service Attack

Description / Impact

Microsoft

- A vulnerability in the Microsoft Malware Protection Engine could allow a remote attacker to execute arbitrary code on the system.
- Affected Systems: **Microsoft Windows Defender, Microsoft Security Essentials, Microsoft Forefront Endpoint Protection 2010, Microsoft Exchange Server 2016, Microsoft Endpoint Protection, Microsoft Forefront Endpoint Protection, Microsoft Intune Endpoint Protection, Microsoft Exchange Server 2013**
- Officially Acknowledged by the Vendor: **Yes**

OpenSSL

- A vulnerability in OpenSSL could allow a remote attacker to bypass security restrictions.
- Affected Systems: **OpenSSL 1.0.2**
- Officially Acknowledged by the Vendor: **Yes**

IBM WebSphere

- A vulnerability in the IBM WebSphere MQ could allow a local user to crash the system.
- Affected Systems: **IBM MQ 7.5, IBM MQ 8.0, IBM MQ 9.0 IBM MQ 9.0.1, IBM MQ 9.0.1, IBM MQ 9.0.0.1, IBM MQ 9.0.2, IBM MQ 8.0.0.1, IBM MQ 8.0.0.2, IBM MQ 8.0.0.3, IBM MQ 8.0.0.4, IBM MQ 8.0.0.5, IBM MQ 8.0.0.6, IBM MQ 9.0.3, IBM MQ 7.5.0.1, IBM MQ 7.5.0.2, IBM MQ 7.5.0.3, IBM MQ 7.5.0.4, IBM MQ 7.5.0.5, IBM MQ 7.5.0.6, IBM MQ 7.5.0.7, IBM MQ 7.5.0.8**
- Officially Acknowledged by the Vendor: **Yes**

Risk Reduction Recommendations

Visit the links below and follow the instructions given by respective vendors.

Microsoft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11940
OpenSSL	https://www.openssl.org/news/secadv/20171207.txt
IBM WebSphere	http://www-01.ibm.com/support/docview.wss?uid=swg22005392&cm_mc_uid=06904596679215089083768&cm_mc_sid_50200000=1513052783&cm_mc_sid_51860000=1513052783&cm_mc_sid_50200000=1513052783

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.