1 Vulnerability in Triple-DES (CVE-2016-2183) on z/VSE

Summary

The SWEET32 vulnerability on Triple-DES affects OpenSSL on IBM z/VSE.

Vulnerability Details

CVEID: CVE-2016-2183

DESCRIPTION: SWEET32 (https://sweet32.info) is an attack on older block cipher algorithms that use a block size of 64 bits. In mitigation for the SWEET32 attack DES based ciphersuites have been moved from the HIGH cipherstring group to MEDIUM in OpenSSL 1.0.1 and OpenSSL 1.0.2. OpenSSL 1.1.0 since release has had these ciphersuites disabled by default.

CVSS Base Score: 5.3 (Medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Affected Products and Versions

OpenSSL on z/VSE was affected if using GSK_HIGH_SECURITY in *gsk_get_cipher_info()*. Following APARs move the TDES cipher suite (0x0A) to GSK_LOW_SECURITY:

- DY47688 with PTF UD54209 (z/VSE 5.2)
- DY47689 with PTF UD54211 (z/VSE 6.1)

Remediation/Fixes

GSK_LOW_SECURITY should not be used.

More information

You can find more information on these web sites:

National Vulnerability Database (NVD)
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183

Vulnerability Summary for CVE-2015-7575
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2183