1 Vulnerability in MD5 Signature and Hash Algorithm (CVE-2015-7575) on z/VSE

Summary

The MD5 “SLOTH” vulnerability on TLS 1.2 affects OpenSSL on IBM z/VSE.

Vulnerability Details

CVEID: CVE-2015-7575

DESCRIPTION: The TLS protocol could allow weaker than expected security caused by a collision attack when using the MD5 hash function for signing a ServerKeyExchange message during a TLS handshake. An attacker could exploit this vulnerability using man-in-the-middle techniques to impersonate a TLS server and obtain credentials.

CVSS Base Score: 7.1
CVSS Temporal Score: See https://exchange.xforce.ibmcloud.com/vulnerabilities/109415 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N)

Affected Products and Versions

OpenSSL on z/VSE is affected if using GSK_LOW_SECURITY in *gsk_get_cipher_info()*. Only in this case SSL cipher suite 01 (NULL-MD5) is available for backward compatibility with old applications.

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-2015-7575

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