Micro Focus Security Update

Universal CMDB

CVE-2016-6329 Sweet32: Birthday attacks on 64-bit block ciphers in TLS

Document management:

Date	Version	Change
September 18, 2017	Version 1.0	Initial release

Summary:

The following article enlists the necessary related details on the Micro Focus Product Universal CMDB on the Sweet32: Birthday attacks on 64-bit block ciphers in TLS CVE-2016-6329.

Topic

OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTP-over-OpenVPN session using Blowfish in CBC mode, aka a "Sweet32" attack.

Reference's links (Nist if existing)

***Note**: This link provides further information about this issue and lists the Samba versions affected.*

Affected Releases:

The following versions of Universal CMDB were found vulnerable:

UCMDB 10.10 / 10.11
UCMDB 10.20 / 10.21 / 10.22
UCMDB 10.30 / 10.31
UCMDB Browser for Universal CMDB 4.10 / 4.11

Response

ACTION: Review all details in instructions provided in this paper to address the vulnerability.
Micro Focus recommend addressing this information as soon as possible.

Impact on Universal CMDB

The Universal CMDB Server component of UCMDB, is affected.
The Universal Discovery Probe component is affected.
The UD Content Pack component of UCMDB, is affected.
The UCMDB Browser component is affected.

The secure communication between UCMDB Server and UCMDB Probe/UD Agent, UCMDB Server and UCMDB Browser is affected by the Sweet32 Birthday attack, in this way an attacker can alter the communication between endpoints and get the data in clear text.

Mitigation Actions

Micro Focus has released the following software updates to resolve the vulnerability for the impacted versions of Universal CMDB:

Note: Micro Focus recommends installing the latest software updates, if possible. Customers unable to apply the updates should contact Micro Focus Support to discuss options.

Affected versions	Solution	
UCMDB 10.10, 10.11	UCMDB 10.11 CUP9 or later Windows: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00194 Linux: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00195 UD Content Pack 22 | Version 22.00 https://hpln.hpe.com/contentoffering/ud-content-packs **Please, contact support for getting the hotfix.**	
UCMDB 10.20, 10.21, 10.22	UCMDB 10.22 CUP6 or later Windows: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00198 Linux: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00199 UD Content Pack 23 | Version 23.00 https://hpln.hpe.com/contentoffering/ud-content-packs	

UCMDB 10.30, 10.31	UCMDB 10.32 or later **Windows:** Software Entitlements Portal **Linux:** Software Entitlements Portal UD Content Pack 23 | Version 23.00 or later **https://hpln.hpe.com/contentoffering/ud-content-packs**	
UCMDB Browser 4.10, 4.11	UCMDB Browser 4.12 or later **ITOM Marketplace**	