MICRO FOCUS

Micro Focus Security Update

Universal CMDB
Installation File Access Control Privilege on Windows

Document management:

Date	Version	Change
March 26, 2018	Version 1.0	Initial release

Summary:

The following article enlists the necessary related details on the Micro Focus Product Universal CMDB on the Installation File Access Control Privilege on Windows system.

Topic

Universal CMDB allows file access permissions for all the users.

Affected Releases:

The following versions of Universal CMDB were found vulnerable:

> UCMDB 10.20 / 10.21 / 10.22
> UCMDB 10.30 / 10.31 / 10.32 / 10.33
> UCMDB 11.0

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.

MICRO FOCUS®

Impact on Universal CMDB

The Universal CMDB Server component of UCMDB is affected.
The Universal Discovery Probe component of UCMDB is affected.

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 10.20; 10.21; 10.22	UCMDB 10.22 CUP6 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** Run steps as described below	
UCMDB 10.30; 10.31; 10.32; 10.33	UCMDB 10.33 CUP1 Windows: **https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00200** Linux: **https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00201** Run steps as described below	
UCMDB 11.0	Run steps as described below	

Solution for mitigate the vulnerability in affected versions UCMDB 10.2x, UCMDB 10.3x, UCMDB 11.0

If you use UCMDB version 10.22 CUP6, 10.33 CUP1, 11.0 follow the steps as described below in order to mitigate the vulnerability.

1. Remove the users group assess privilege from UCMDB Server install folder on windows system. Below, there are command samples for reference:

MICRO FOCUS®

a. ICACLS commands 'icacls <user_installdirt> /inheritace:d', 'icalcs <user_installdir> /remove:g Users';

b. CACLS commands 'cacls <user_installdir> /T /E /R Users'