



CVE-2018-6496

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-6496
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-16 01:29:00 UTC
Updated	2023-11-07 02:59:00 UTC
Description	Remote Cross-site Request forgery (CSRF) potential has been identified in UCMBD Browser version 4.10, 4.11, 4.12, 4.13

Risk And Classification

Problem Types: CWE-352 | CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microfocus	Universal Cmbd Browser	All	All	All	All

References

Reference

- HP UCMDB Browser CVE-2018-6496 Cross Site Request Forgery Vulnerability
- MFSBGN03809 rev.1 - Universal CMDB, Deserialization Java Objects and CSRF - , universal cmbd - other - Micro Focus Software Support
- Micro Focus Universal Configuration Management Database Browser Lets Remote Users Conduct Cross-Site Request Forgery and Object De
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Micro Focus would like to thank Mateusz Garncarek for reporting this issue to cyber-psrt@microfocus.com.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)