CVE-2018-18591

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-18591
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-13 13:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	A potential unauthorized disclosure of data vulnerability has been identified in Micro Focus Service Manager versions: 9.30,

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microfocus	Service Manager	9.30	All	All	All
Application	Microfocus	Service Manager	9.31	All	All	All
Application	Microfocus	Service Manager	9.32	All	All	All
Application	Microfocus	Service Manager	9.33	All	All	All
Application	Microfocus	Service Manager	9.34	All	All	All
Application	Microfocus	Service Manager	9.35	All	All	All
Application	Microfocus	Service Manager	9.40	All	All	All
Application	Microfocus	Service Manager	9.41	All	All	All
Application	Microfocus	Service Manager	9.50	All	All	All
Application	Microfocus	Service Manager	9.51	All	All	All
Application	Microfocus	Service Manager	9.30	All	All	All
Application	Microfocus	Service Manager	9.31	All	All	All
Application	Microfocus	Service Manager	9.32	All	All	All
Application	Microfocus	Service Manager	9.33	All	All	All
Application	Microfocus	Service Manager	9.34	All	All	All
Application	Microfocus	Service Manager	9.35	All	All	All
Application	Microfocus	Service Manager	9.40	All	All	All

Application	Microfocus	Service Manager	9.41	All	All	All
Application	Microfocus	Service Manager	9.50	All	All	All
Application	Microfocus	Service Manager	9.51	All	All	All

References

Reference	Source	Link	Tags
MySupport - Micro Focus Software Support		softwaresupport.softwaregrp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**