



CVE-2020-3158

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-3158
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-19 20:15:00 UTC
Updated	2020-02-28 00:47:00 UTC
Description	A vulnerability in the High Availability (HA) service of Cisco Smart Software Manager On-Prem could allow an unauthenticated

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Smart Software Manager On-prem	All	All	All	All
Application	Cisco	Smart Software Manager On-prem	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Smart Software Manager On-Prem Static Default Credential Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
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.

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