Cisco Smart Software Manager On-Prem Privilege Escalation Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-20151
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 17:28:31 UTC
Updated	2026-04-01 17:28:31 UTC
Description	A vulnerability in the web interface of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticate

Risk And Classification

Primary CVSS: v3.1 7.3 HIGH from psirt@cisco.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

Problem Types: CWE-201 | CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSSV3_1	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 7-202001	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202004	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202006	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202012	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202010	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202008	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202201	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202102	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202105	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202108	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202112	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202201	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202206	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202212	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202302	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202303	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202304	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202308	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202401	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 8-202404	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202406	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202407	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202410	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202412	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202501	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202502	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202504	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202507	Not specified
CNA	Cisco	Cisco Smart Software Manager On-Prem	affected 9-202510	Not specified

References

Reference	Source	Link	Ta
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-p...	psirt@cisco.com	sec.cloudapps.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Exploits

CNA: The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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