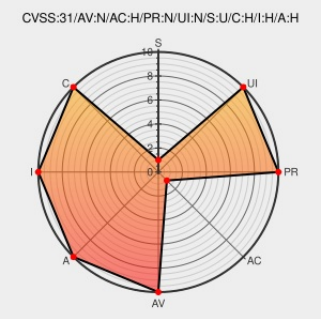
CVE-2020-27131

Published on: 11/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:27 PM UTC

CVE-2020-27131 - advisory for cisco-sa-csm-java-rce-mWJEedcD

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Security Manager from Cisco contain the following vulnerability:

Multiple vulnerabilities in the Java deserialization function that is used by Cisco Security Manager could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected device. These vulnerabilities are due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit these vulnerabilities by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary commands on the device with the privileges of NT AUTHORITY\SYSTEM on the Windows target host. Cisco has not released software updates that address these vulnerabilities.

CVE-2020-27131 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

The Cisco Product Security Incident Response Team (PSIRT) is aware of public announcements about these vulnerabilities. Cisco PSIRT is not aware of malicious use of the vulnerabilities that are described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Security Manager** version **n/a**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Security Manager Java Deserialization Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20201116 Cisco Security Manager Java Deserialization Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Security Manager	All	All	All	All

cpe:2.3:a:cisco:security_manager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@pwnwikiorg	CVE-2020-27131 Cisco Security Manager 反序列化RCE漏洞 pwnwiki.org/index.php?titl…	2021-04-27 07:00:22

← Previous ID

Next ID→