CVE-2020-6287

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

Summary

CVE	CVE-2020-6287
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-14 13:15:00 UTC
Updated	2022-04-28 18:57:00 UTC
Description	SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication

Risk And Classification

EPSS: 0.943620000 probability, percentile 0.999620000 (date 2026-04-06)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-306

CISA Known Exploited Vulnerability

Vendor	SAP
Product	NetWeaver
Name	SAP NetWeaver Missing Authentication for Critical Function Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-6287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Application Server Java	7.30	All	All	All
Application	Sap	Netweaver Application Server Java	7.31	All	All	All
Application	Sap	Netweaver Application Server Java	7.40	All	All	All
Application	Sap	Netweaver Application Server Java	7.50	All	All	All
Application	Sap	Netweaver Application Server Java	7.30	All	All	All
Application	Sap	Netweaver Application Server Java	7.31	All	All	All
Application	Sap	Netweaver Application Server Java	7.40	All	All	All
Application	Sap	Netweaver Application Server Java	7.50	All	All	All

References

Reference
launchpad.support.sap.com
Full Disclosure: Onapsis Security Advisory 2021-0003: [CVE-2020-6287] - [SAP RECON] SAP JAVA: Unauthenticated execution of configurat
SAP RECON Cybersecurity Vulnerability | Onapsis
SAP Security Patch Day – July 2020 - Product Security Response at SAP - Community Wiki
SAP JAVA Configuration Task Execution ≈ Packet Storm
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

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