



CVE-2020-12712

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

Summary

CVE	CVE-2020-12712
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-11 14:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	A vulnerability based on insecure user/password encryption in the JOE (job editor) component of SOS JobScheduler 1.12 a

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sos-berlin	Jobscheduler	All	All	All	All
Application	Sos-berlin	Jobscheduler	All	All	All	All

References

Reference	Source	Link	Tags
[JOE-290] Password Obfuscation Vulnerability (CVE-2020-12712) - SOS JIRA	CONFIRM	change.sos-berlin.com	Vendor Advisor
Vulnerability Release 1.13.4 - Product Knowledge Base - Product Knowledge Base	MISC	kb.sos-berlin.com	Release Notes,
News	MISC	www.sos-berlin.com	Vendor Advisor
SOS JobScheduler 1.13.3 Stored Password Decryption ~ Packet Storm	MISC	packetstormsecurity.com	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)