CVE-2019-3698

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

Summary

CVE	CVE-2019-3698
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-28 14:15:00 UTC
Updated	2021-09-14 12:39:00 UTC
Description	UNIX Symbolic Link (Symlink) Following vulnerability in the cronjob shipped with nagios of SUSE Linux Enterprise Server 1

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagios	Nagios	All	All	All	All
Application	Nagios	Nagios	All	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:0517-1: moderate: Security update f	SUSE	lists.op
Bug 1156309 – VUL-0: CVE-2019-3698: nagios: /etc/cron.weekly/nagios allows privilege escalation from nagios to root	CONFIRM	bugzilla
[security-announce] openSUSE-SU-2020:0500-1: moderate: Security update f	SUSE	lists.op
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

Vendor Comments And Credit

Discovery Credit

LEGACY: Matthias Gerstner

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