CVE-2022-48321

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

Summary

CVE	CVE-2022-48321
State	PUBLIC
Assigner	security@checkmk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-20 17:15:00 UTC
Updated	2024-01-09 02:10:00 UTC
Description	Limited Server-Side Request Forgery (SSRF) in agent-receiver in Tribe29's Checkmk <= 2.1.0p11 allows an attacker to cor

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tribe29	Checkmk	2.1.0	-	All	All
Application	Tribe29	Checkmk	2.1.0	b1	All	All
Application	Tribe29	Checkmk	2.1.0	b2	All	All
Application	Tribe29	Checkmk	2.1.0	b3	All	All
Application	Tribe29	Checkmk	2.1.0	b4	All	All
Application	Tribe29	Checkmk	2.1.0	b5	All	All
Application	Tribe29	Checkmk	2.1.0	b6	All	All
Application	Tribe29	Checkmk	2.1.0	b7	All	All
Application	Tribe29	Checkmk	2.1.0	b8	All	All
Application	Tribe29	Checkmk	2.1.0	b9	All	All
Application	Tribe29	Checkmk	2.1.0	p1	All	All
Application	Tribe29	Checkmk	2.1.0	p10	All	All
Application	Tribe29	Checkmk	2.1.0	p11	All	All
Application	Tribe29	Checkmk	2.1.0	p2	All	All
Application	Tribe29	Checkmk	2.1.0	p3	All	All
Application	Tribe29	Checkmk	2.1.0	p4	All	All
Application	Tribe29	Checkmk	2.1.0	p5	All	All

Application	Tribe29	Checkmk	2.1.0	p6	All	All
Application	Tribe29	Checkmk	2.1.0	p7	All	All
Application	Tribe29	Checkmk	2.1.0	p8	All	All
Application	Tribe29	Checkmk	2.1.0	p9	All	All

References

Reference	Source	Link	Tags
Fix limited SSRF in agent-receiver API	MISC	checkmk.com	
Checkmk: Remote Code Execution by Chaining Multiple Bugs (1/3) | Sonar	MISC	www.sonarsource.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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