



CVE-2020-10569

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

Summary

CVE	CVE-2020-10569
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-21 19:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	** DISPUTED ** SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat att

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sysaid	On-premise	20.1.11	All	All	All
Application	Sysaid	On-premise	20.1.11	All	All	All

References

Reference	Source	Link	Tags
Release Notes - On-Premise 20.2 SysAid	MISC	www.sysaid.com	Release Notes, Vendor Advisory
Sysaid 20.1.11 b26 Remote Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VD
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.

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