



CVE-2020-13229

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

Summary

CVE	CVE-2020-13229
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-02 14:15:00 UTC
Updated	2020-06-02 15:11:00 UTC
Description	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi U

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sysax	Multi Server	6.90	All	All	All
Application	Sysax	Multi Server	6.90	All	All	All

References

Reference
Sysax-MultiServer-6.90-Multiple-Vulnerabilities/README.md at master · wrongsid3/Sysax-MultiServer-6.90-Multiple-Vulnerabilities · GitHub
wrongsid3 (Luca Epifanio) · GitHub
CVE Program record
NVD vulnerability detail

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