CVE-2020-15117

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

Summary

CVE	CVE-2020-15117
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-15 18:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	In Synergy before version 1.12.0, a Synergy server can be crashed by receiving a kMsgHelloBack packet with a client nam

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Symless	Synergy	All	All	All	All
Application	Symless	Synergy	All	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 33 Update: synergy-1.12.0-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: synergy-1.12.0-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: synergy-1.12.0-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Denial of Service / Crash of synergys · Advisory · symless/synergy-core · GitHub	CONFIRM	github.com	Thi
[SECURITY] Fedora 33 Update: synergy-1.12.0-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Merge pull request from GHSA-chfm-333q-gfpp · symless/synergy-core@0a97c2b · GitHub	MISC	github.com	Pat
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**