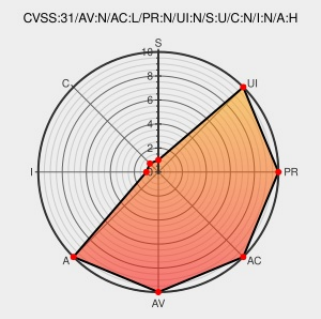
CVE-2021-21404

Published on: 04/06/2021 12:00:00 AM UTC

Last Modified on: 04/14/2021 06:00:00 PM UTC

CVE-2021-21404 - advisory for GHSA-x462-89pf-6r5h

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Syncthing from Syncthing contain the following vulnerability:

Syncthing is a continuous file synchronization program. In Syncthing before version 1.15.0, the relay server `strelaysrv` can be caused to crash and exit by sending a relay message with a negative length field. Similarly, Syncthing itself can crash for the same reason if given a malformed message from a malicious relay server when attempting to join the relay. Relay joins are essentially random (from a subset of low latency relays) and Syncthing will by default restart when crashing, at which point it's likely to pick another non-malicious relay. This flaw is fixed in version 1.15.0.

CVE-2021-21404 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **syncthing** - **syncthing** version **< 1.15.0**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

CVE References

Description	Tags	Link
Release v1.15.0 · syncthing/syncthing · GitHub	github.com text/html	MISC github.com/syncthing/syncthing/releases/tag/v1.15.0
syncthing · pkg.go.dev	pkg.go.dev text/html	MISC pkg.go.dev/github.com/syncthing/syncthing
Merge pull request from GHSA-x462-89pf-6r5h · syncthing/syncthing@fb4fdaf · GitHub	github.com text/html	MISC github.com/syncthing/syncthing/commit/fb4fdaf4c0a79c22cad000c42ac1394e3ccb6a97
Crash due to malformed relay protocol message · Advisory · syncthing/syncthing · GitHub	github.com text/html	CONFIRM github.com/syncthing/syncthing/security/advisories/GHSA-x462-89pf-6r5h

Related QID Numbers

180256 Debian Security Update for syncthing (CVE-2021-21404)

501696 Alpine Linux Security Update for syncthing

501928 Alpine Linux Security Update for syncthing

690173 Free Berkeley Software Distribution (FreeBSD) Security Update for syncthing (9ee01e60-6045-43df-98e5-a794007e54ef)

750224 OpenSUSE Security Update for syncthing (openSUSE-SU-2021:0688-1)

982429 Go (go) Security Update for github.com/syncthing/syncthing (GHSA-x462-89pf-6r5h)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Syncthing	Syncthing	All	All	All	All

cpe:2.3:a:syncthing:syncthing:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-21404 : Syncthing is a continuous file synchronization program. In Syncthing before version 1.15.0, the re… twitter.com/i/web/status/1…	2021-04-06 20:07:24
/r/netcve	CVE-2021-21404	2021-04-06 20:25:21

← Previous ID

Next ID→

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