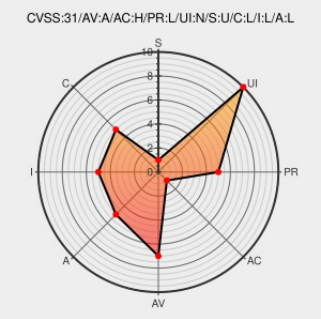
CVE-2020-36617

Published on: Not Yet Published

Last Modified on: 12/22/2022 07:45:00 PM UTC

CVE-2020-36617

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



Certain versions of Sftpserver from Greenend contain the following vulnerability:

** DISPUTED ** A vulnerability was found in ewxrjk sftpserver. It has been declared as problematic. Affected by this vulnerability is the function sftp_parse_path of the file parse.c. The manipulation leads to uninitialized pointer. The real existence of this vulnerability is still doubted at the moment. The name of the patch is bf4032f34832ee11d79aa60a226cc018e7ec5eed. It is recommended to apply a patch to fix this issue. The identifier VDB-216205 was assigned to this vulnerability. NOTE: In some deployment models this would be a vulnerability. README specifically warns about avoiding such deployment models.

CVE-2020-36617 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ewxrjk** - **sftpserver** version **n/a**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
CVE-2020-36617 | ewxrjk sftpserver parse.c sftp_parse_path uninitialized pointer	vuldb.com text/html	MISC vuldb.com/?id.216205
Fix handle mis-parse · ewxrjk/sftpserver@bf4032f · GitHub	github.com text/html	MISC github.com/ewxrjk/sftpserver/commit/bf4032f34832ee11d79aa60a226cc018e7ec5eed

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Greenend	Sftpserver	All	All	All	All

cpe:2.3:a:greenend:sftpserver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-36617 : ** DISPUTED ** A vulnerability was found in ewxrjk sftpserver. It has been declared as problematic… twitter.com/i/web/status/1…	2022-12-18 15:09:36
/r/netcve	CVE-2020-36617	2022-12-18 15:38:36

← Previous ID

Next ID→