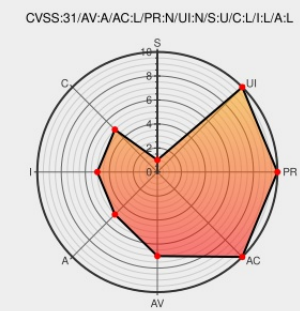
CVE-2020-9291

Published on: 06/01/2020 12:00:00 AM UTC

Last Modified on: 04/20/2021 05:31:00 PM UTC

CVE-2020-9291

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



Certain versions of Forticlient from Fortinet contain the following vulnerability:

An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack.

CVE-2020-9291 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiClient for Windows** version **FortiClient for Windows 6.2.1 and earlier and FortiClient for Windows 6.0.9 and earlier**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
FortiClient for Windows Insecure Temporary File vulnerability | FortiGuard	Vendor Advisory fortiguard.com	MISC fortiguard.com/psirt/FG-IR-20-040

		text/html
FortiClient for Windows Insecure Temporary File vulnerability | FortiGuard	Vendor Advisory www.fortiguard.com text/html	MISC www.fortiguard.com/psirt/FG-IR-20-040

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	Fortinet	Forticlient	All	All	All	All
Application	Fortinet	Forticlient	All	All	All	All

cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:windows:*:*:

cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→