



CVE-2021-27406

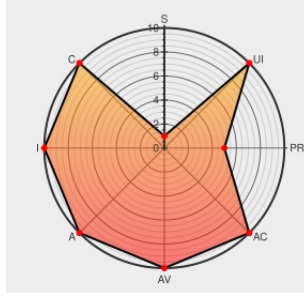
Published on: Not Yet Published

Last Modified on: 10/18/2022 01:38:00 PM UTC

CVE-2021-27406

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Openvpn-client](#) from [Perfact](#) contain the following vulnerability:

An attacker can take leverage on PerFact OpenVPN-Client versions 1.4.1.0 and prior to send the config command from any application running on the local host machine to force the back-end server into initializing a new open-VPN instance with arbitrary open-VPN configuration. This could result in the attacker achieving execution with privileges of a SYSTEM user.

CVE-2021-27406 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [PerFact](#) - **OpenVPN-Client** version **<= 1.4.1.0**

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
PerFact OpenVPN-Client CISA	www.cisa.gov text/html	CONFIRM www.cisa.gov/uscert/ics/advisories/icsa-21-056-01

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.

Related QID Numbers

Exploit/POC from Github

An attacker can take leverage on PerFact OpenVPN-Client versions 1.4.1.0 and prior to send the config command from an...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Perfact	Openvpn-client	All	All	All	All
cpe:2.3:a:perfect:openvpn-client:*****::						

Discovery Credit

Sharon Brizinov of Claroty reported this vulnerability to CISA.

Social Mentions

Source	Title	Posted (UTC)
 @CSTOOL_io	"Code Execution Vulnerabilities Affect OpenVPN-Based Applications", including Siemens products: attacksrfc.cstool.io/cve/CVE-2021-2...	2021-11-23 07:39:09
 @cybermindy	@Claroty Cool research! Would anyone know why CVE-2021-27406 does not have a NIST entry? It was reserved in February, still no details	2021-11-26 18:52:42
 @CVEreport	CVE-2021-27406 : An attacker can take leverage on PerFact OpenVPN-Client versions 1.4.1.0 and prior to send the con... twitter.com/i/web/status/1...	2022-10-14 17:06:15
 /r/netcve	CVE-2021-27406	2022-10-14 18:38:56

[← Previous ID](#)[Next ID →](#)