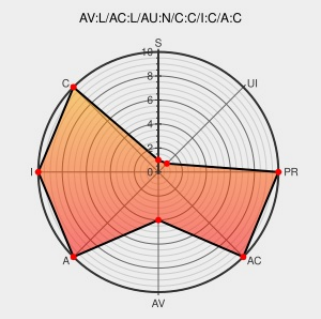
CVE-2015-5736

Published on: 09/03/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5736

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



Certain versions of Forticlient from Fortinet contain the following vulnerability:

The Fortishield.sys driver in Fortinet FortiClient before 5.2.4 allows local users to execute arbitrary code with kernel privileges by setting the callback function in a (1) 0x220024 or (2) 0x220028 ioctl call.

CVE-2015-5736 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
FortiClient Antivirus Information Exposure / Access Control ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/133398/FortiClient-Antivirus-Information-Exposure-Access-Control.html
Fortinet FortiClient 5.2.3 (Windows 10 x64 Pre-Anniversary) - Local Privilege Escalation - Windows_x86-64 local Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 41721
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20150901 [CORE-2015-0013] - FortiClient Antivirus Multiple Vulnerabilities
Fortinet FortiClient Bugs Let Local Users View Memory Contents, Modify the Registry, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1033439

FortiGuard.com | Mulitple Vulnerabilities in FortiClient	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.fortiguard.com/advisory/mulitple-vulnerabilities-in-forticlient
Full Disclosure: [CORE-2015-0013] - FortiClient Antivirus Multiple Vulnerabilities	seclists.org text/html	FULLDISC 20150901 [CORE-2015-0013] - FortiClient Antivirus Multiple Vulnerabilities
Fortinet FortiClient 5.2.3 (Windows 10 x64 Creators) - Local Privilege Escalation	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 45149
FortiGuard.com | Mulitple Vulnerabilities in FortiClient	fortiguard.com text/html	CONFIRM fortiguard.com/advisory/mulitple-vulnerabilities-in-forticlient
Fortinet FortiClient 5.2.3 (Windows 10 x64 Post-Anniversary) - Local Privilege Escalation - Windows_x86-64 local Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 41722
FortiClient Antivirus Multiple Vulnerabilities | CORE Security	www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/forticlient-antivirus-multiple-vulnerabilities

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→