

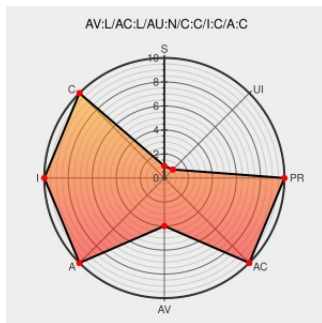


CVE-2015-5736

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 [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

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

SECTRAK 1033439

FortiGuard.com Multiple Vulnerabilities in FortiClient	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.fortiguards.com/advisory/multiple-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 Multiple Vulnerabilities in FortiClient	fortiguards.com text/html	 CONFIRM fortiguards.com/advisory/multiple-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

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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