



CVE-2017-14961

Published on: 11/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14961

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

Certain versions of [Anti.virus](#) from [Ikarussecurity](#) contain the following vulnerability:

In IKARUS anti.virus 2.16.7, the ntguard.sys driver contains an Arbitrary Write vulnerability because of not validating input values from IOCTL 0x8300000c.

CVE-2017-14961 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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: **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
IKARUS anti.virus 2.16.7 - 'ntguard_x64' Local Privilege Escalation - Windows_x86-64 local Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43139

IKARUS AntiVirus 2.16.7 Privilege Escalation ≈ Packet Storm

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

📄 MISC

packetstormsecurity.com/files/144955/IKARUS-AntiVirus-2.16.7-Privilege-Escalation.html

The Evil Bit Blog: Turning CVE-2017-14961 (IKARUS anti.virus local kernel exploit) into full arbitrary read / write with PALETTE objects

Exploit

Third Party Advisory

theevilbit.blogspot.co.uk

text/html

🌐 MISC

theevilbit.blogspot.co.uk/2017/11/turning-cve-2017-14961-ikarus-antivirus.html

Page not found – IKARUS Security Software

Vendor Advisory

www.ikarussecurity.com

text/html

Inactive Link

Not Archived

🚩 CONFIRM

www.ikarussecurity.com/about-ikarus/security-blog/vulnerability-in-windows-antivirus-products-ik-sa-2017-0002/

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	ikarussecurity	Anti.virus	2.16.7	All	All	All
Application	ikarussecurity	Anti.virus	2.16.7	All	All	All

cpe:2.3:a:ikarussecurity:anti.virus:2.16.7:*:*:*:*:*:

cpe:2.3:a:ikarussecurity:anti.virus:2.16.7:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→