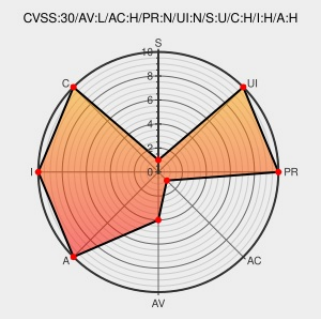
CVE-2017-15643

Published on: 10/19/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15643

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



Certain versions of Ikarus Antivirus from Ikarussecurity contain the following vulnerability:

An active network attacker (MiTM) can achieve remote code execution on a machine that runs IKARUS Anti Virus 2.16.7. IKARUS AV for Windows uses cleartext HTTP for updates along with a CRC32 checksum and an update value for verification of the downloaded files. The attacker first forces the client to initiate an update transaction by modifying an update field within an HTTP 200 response, so that it refers to a nonexistent update. The attacker then modifies the HTTP 404 response so that it specifies a successfully found update, with a Trojan horse executable file (e.g., guardxup.exe) and the correct CRC32 checksum for that file.

CVE-2017-15643 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.4 - HIGH

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

CVSS2 Score: 7.6 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Page not found – IKARUS Security Software	Vendor Advisory www.ikarussecurity.com text/html Inactive Link Not Archived	MISC www.ikarussecurity.com/about-ikarus/security-blog/vulnerability-in-windows-antivirus-products-ik-sa-2017-0001/
401 Authorization Required	Exploit Technical Description Third Party Advisory blogs.securiteam.com text/html Inactive Link Not Archived	MISC blogs.securiteam.com/index.php/archives/3485

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	Ikarus Antivirus	2.16.7	All	All	All
Application	Ikarussecurity	Ikarus Antivirus	2.16.7	All	All	All

cpe:2.3:a:ikarussecurity:ikarus_antivirus:2.16.7:*:*:*:*:*:*:*:

cpe:2.3:a:ikarussecurity:ikarus_antivirus:2.16.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→