



Avira Internet Security Arbitrary File Deletion via Improper Link Resolution

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2026-27748
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-05 15:16:11 UTC
Updated	2026-04-01 15:22:35 UTC
Description	Avira Internet Security contains an improper link resolution vulnerability in the Software Updater component. During the up

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

EPSS: 0.000160000 probability, percentile 0.036350000 (date 2026-04-01)

Problem Types: CWE-59 | CWE-59 CWE-59 Improper Link Resolution Before File Access ('Link Following')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
3.1	security@nortonlifelock.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avira	Internet Security	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gen Digital Inc.	Avira Internet Security	affected 1.1.109.1990 semver	Windows
CNA	Gen Digital Inc.	Avira Internet Security	unaffected 1.1.114.3113 semver	Windows

References

Reference	Source	Link	Tags
www.gendigital.com/us/en/contact-us/security-advisories	security@nortonlifelock.com	www.gendigital.com	
www.avira.com/en/internet-security	security@nortonlifelock.com	www.avira.com	Product
support.avira.com/hc/en-us/articles/360010656158-Current-Avira-versions	security@nortonlifelock.com	support.avira.com	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, primary

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade Avira Internet Security for Windows to version 1.1.114.3113 or later. Apply updates through the product's built-in updater or a fresh install from the vendor; see the release-notes reference in this record for current supported versions.

There are currently no legacy QID mappings associated with this CVE.

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](#)