CVE-2026-8398

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-8398
State	PUBLISHED
Assigner	Kaspersky
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 09:16:17 UTC
Updated	2026-05-15 09:16:17 UTC
Description	A supply chain attack compromised the official installation packages of DAEMON Tools Lite (Windows versions 12.5.0.242

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from vulnerability@kaspersky.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-506 | CWE-506 CWE-506: Embedded Malicious Code

Version	Source	Type	Score	Severity	Vector
4.0	vulnerability@kaspersky.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N
3.1	vulnerability@kaspersky.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AVB Disc Soft	DAEMON Tools Lite	affected 12.5.0.2421 2.6.0.* semver	Windows

References

Reference	Source	Link	Tags
securelist.com/tr/daemon-tools-backdoor/119654	vulnerability@kaspersky.com	securelist.com	
blog.daemon-tools.cc/post/security-incident	vulnerability@kaspersky.com	blog.daemon-tools.cc	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Igor Kuznetsov (Kaspersky) (en)

CNA: Georgy Kucherin (Kaspersky) (en)

CNA: Leonid Bezvershenko (Kaspersky) (en)

CNA: Anton Kargin (Kaspersky) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-06T00:00:00.000Z	Advisory published by vendor

Solutions

CNA: Users of potentially infected application are recommended to uninstall the application, run a full system scan using antivirus software with the latest version of the anti-virus databases, and install the latest version of DAEMON Tools Lite (12.6 or newer) from the official website.

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