

# CVE-2026-8398

## Daemon Tools Lite Embedded Malicious Code Vulnerability

CISA KEV since May 27, 2026

Actively exploited

A supply chain attack compromised the official installation packages of DAEMON Tools Lite (Windows versions 12.5.0.2421 through 12.5.0.2434), distributed from the legitimate website daemon-tools.cc between approximately April 8, 2026, and May 5, 2026. Attackers gained unauthorized access to the vendor's (AVB Disc Soft) build or distribution infrastructure and trojanized three binaries: DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe.

|                                                                     |                                                  |                                                          |                                                                                            |
|---------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>75</b> / <sub>100</sub><br><b>Urgent</b> priority | <b>CVSS V4.0</b><br><b>9.3</b><br>Critical · NVD | <b>EPSS</b><br><b>0.010</b><br>61.2nd percentile · FIRST | <b>CISA DEADLINE</b><br><b>May 30, 2026</b><br>CISA federal deadline · Overdue by 5 months |
|---------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                        |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|----------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild     |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last year |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.010 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable          |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 9.3                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                    |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

These files were digitally signed with the legitimate AVB Disc Soft code-signing certificate, allowing the malicious installers to appear trustworthy and bypass signature-based detection.

### Affected and fixed versions

| PACKAGE      | AFFECTED | FIXED IN                | SOURCE |
|--------------|----------|-------------------------|--------|
| daemon tools | 12.5.1   | no fixed version listed | NVD    |
| windows      | —        | no fixed version listed | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-rm3r-35x9-jv93](https://github.com/advisories/GHSA-rm3r-35x9-jv93)  
**NVD** [nvd.nist.gov/vuln/detail/CVE-2026-8398](https://nvd.nist.gov/vuln/detail/CVE-2026-8398)

**Additional guidance** [blog.daemon-tools.cc/post/security-incident](https://blog.daemon-tools.cc/post/security-incident)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2026-30514](https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-30514)

**Current data** [evulnable.com/vulnerability-management/cve/CVE-2026-8398](https://evulnable.com/vulnerability-management/cve/CVE-2026-8398)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.