contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

SolarWinds Dameware: new CVE

CVE-2026-28336 · record published 3 November 2026

Analysis Report

Anyone running SolarWinds Dameware 2026.3 or earlier needs to act: the vendor's advisory, published 3 November 2026, recommends upgrading to version 2026.3.1 as soon as is practical. Start by …

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/solarwinds-dameware-cve-2026-28336

Correction, 5 November 2026: an earlier version of this note described the last affected version as the first version that is not affected. The CVE record lists that version as affected. Read the vendor's page for the release that fixes it before you decide that you are safe.

The bottom line

> *Anyone running SolarWinds Dameware 2026.3 or earlier needs to act: the vendor's advisory, published 3 November 2026, recommends upgrading to version 2026.3.1 as soon as is practical. Start by confirming which version is installed across every host running Dameware.*

At a glance

Fact	Detail
Product	SolarWinds Dameware (CVE-2026-28336)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by SolarWinds on 3 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 5 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	SolarWinds Dameware 2026.3.1 (vendor's advisory published 3 November 2026).
Who looks first	Any organisation using SolarWinds Dameware on version 2026.3 or earlier. The vendor's advisory lists all versions up to and including 2026.3 as affected, so any installation not yet on 2026.3.1 is in scope.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SolarWinds Dameware (Mini Remote Control or Remote Support)?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version 2026.3 or earlier?	You are on 2026.3.1 or later; nothing further to do.	Your installation is in the affected range; continue.
Can anyone with a Dameware account reach the server over the network?	Exposure is limited; still plan to upgrade at next maintenance.	Prioritise upgrading to 2026.3.1 promptly.

What it is

The record says an authenticated Dameware user can inject commands that the product then runs on the host being remotely controlled, potentially giving an attacker full control of that machine. Only a low-privilege account is needed; no technical complexity and no help from anyone else is required.

What the vendor's advisory says

We read two pages on documentation.solarwinds.com and www.solarwinds.com. In short:

- The same 2026.3.1 release also fixes CVE-2026-28335 (8.4 High): a buffer overflow in Dameware that the advisory says can result in remote code execution; authentication is required.
- CVE-2026-28327 (8.2 High) is fixed in the same release: a DLL hijacking that occurs during installation only and requires local machine access and admin privileges.
- Third-party component: CVE-2026-111497 (9.8 Critical), a buffer overflow in Brotli decoder versions 1.0.3 through 1.2.0; the advisory says to update to version 1.0.10, 1.1.1, or 1.2.1.
- Third-party component: CVE-2026-40021 (6.3 Medium), Apache Log4net XmlLayout before version 3.3.0 fails to sanitise certain characters, allowing log records to be suppressed; fixed in Log4net 3.3.0.
- The release notes say Dameware Remote Support 12.2.4 and later changed the saved hosts protection mechanism; back up DRS registry settings and saved hosts before upgrading from an earlier version.

Things people will get wrong

- Authentication is required, so an external attacker cannot exploit this. The CVSS vector shows low privilege (PR:L) is sufficient — not admin, just any valid account. A compromised or malicious user with a Dameware login can attempt this over the network.
- Only the Dameware software itself is at risk. The record says the attack can lead to compromise of the remotely controlled host, not just Dameware. The CVSS scope is changed (S:C), confirming impact can extend beyond the Dameware component.

How we would triage it

This is our judgement.

Step 1: Find the version installed on each host

- Run the command below on each Windows host where Dameware may be installed; the vendor's advisory says all versions up to and including 2026.3 are affected.

- Check for both Dameware Mini Remote Control and Dameware Remote Support, as the vendor's advisory covers the Dameware product broadly.

Step 2: Reduce exposure if you cannot patch immediately

- Restrict Dameware access to the minimum number of accounts needed; the attack requires an authenticated account, so limiting who can log in reduces the pool of potential sources.
- Isolate the Dameware host from untrusted network segments if upgrading immediately is not possible.

Step 3: Upgrade to SolarWinds Dameware 2026.3.1

- The vendor's advisory says to upgrade to Dameware 2026.3.1 as soon as is practical.
- The release notes say Dameware Remote Support 12.2.4 and later require backing up DRS registry settings and saved hosts before upgrading from an earlier version; complete that step first if applicable.

Step 4: Confirm the upgrade is in place

- Re-run the version check after upgrading to confirm 2026.3.1 is installed on all Dameware hosts.
- Keep a written record of the installed version and the date the upgrade was completed.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of a critical vulnerability in SolarWinds Dameware (CVE-2026-28336), scored 9.9 Critical. The vendor's advisory, published 3 November 2026, states that all versions up to and including 2026.3 are affected and recommends upgrading to version 2026.3.1 as soon as is practical. Could you please confirm whether Dameware is installed in our environment, which version is currently running on each host, and whether the upgrade to 2026.3.1 is in place or planned? Please provide written confirmation of the installed version and the expected date of completion by 12 November 2026. Thank you.*

The weakness behind it

The record classes this as CWE-20.

The sources, in their words

The CVE record:

> *SolarWinds Dameware was found to be affected by a command injection vulnerability that could lead to the compromise of the remotely controlled host. Authentication is required.*

Versions of SolarWinds Dameware the record lists as affected:

- all versions up to and including 2026.3

The record gives no version ranges. Use the vendor's advisory for the affected versions.

What the record says to do about it, in the vendor's words:

> *SolarWinds recommends customers to upgrade to Dameware version 2026.3.1 as soon as is practical.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-28336
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-28336
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say which specific component — Mini Remote Control or Remote Support — contains the command injection flaw, or whether both are equally affected.
- The sources do not describe a workaround for organisations that cannot upgrade to 2026.3.1 immediately.
- The sources do not say whether the vulnerability affects Dameware managed through SolarWinds Orion or any cloud-hosted deployment model.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 5 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-28336: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
3 November 2026	CVE record published by SolarWinds.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Dameware 2026.3 or earlier, reachable from outside the internal network, with active accounts.	Medium	This week.
Dameware 2026.3 or earlier on an internal network with multiple user accounts.	Medium	Within two weeks or next maintenance window.
Dameware 2026.3 or earlier, isolated network, very few accounts, no external access.	Low	Next scheduled patch cycle.
Dameware 2026.3.1 already installed across all hosts.	None	Nothing further for this CVE.
Dameware not installed anywhere in the environment.	None	Nothing to do.

Appendix 4. Definition of done

- Every SolarWinds Dameware you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-28336: https://www.cve.org/CVERecord?id=CVE-2026-28336
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: documentation.solarwinds.com/en/success_center/dameware/content/release_note: https://documentation.solarwinds.com/en/success_center/dameware/content/release_notes/dameware_2026-3-1_release_notes.htm
- Advisory or release notes read: www.solarwinds.com/trust-center/security-advisories/cve-2026-28336: https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28336
- Reference in the CVE record: www.solarwinds.com: https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28336