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 must upgrade to 2026.3.1; the vendor published the fix on 3 November 2026. Start by confirming which version is installed and block external …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 3 November 2026 |
| FACTS AS OF | 3 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

## The bottom line

> *Anyone running SolarWinds Dameware 2026.3 or earlier must upgrade to 2026.3.1; the vendor published the fix on 3 November 2026. Start by confirming which version is installed and block external access to Dameware until the upgrade is complete.*

## 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 3 November 2026, which means nothing public says yet that anyone is using it. |
| Fixed in | SolarWinds Dameware 2026.3.1 (vendor advisory, published 3 November 2026) |
| Who looks first | Any organisation running SolarWinds Dameware 2026.3 or any earlier version. The vendor's advisory says all previous versions are affected. IT providers and administrators who use Dameware to manage remote hosts should check immediately. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run SolarWinds Dameware in your environment? | Nothing to do for this CVE. | Check which version is installed. |
| Is the installed version 2026.3 or any earlier version? | Nothing to do; you are already on the fixed release. | Restrict access and plan the upgrade to 2026.3.1. |
| Can any authenticated Dameware user reach the product over the network? | Lower urgency, but still upgrade at the next opportunity. | Treat as urgent; limit access while arranging the upgrade. |
| Is Dameware reachable from outside your internal network? | Still upgrade promptly; internal users pose sufficient risk. | Block external access immediately, then upgrade. |

## What it is

An authenticated user can inject commands through Dameware that execute on the host being remotely controlled. The vendor's advisory says this could lead to the compromise of that host. The CVSS vector shows the attack travels over the network with low complexity and no further interaction beyond logging in.

## Why it matters

The score of 9.9 reflects the CVSS Changed Scope flag: a successful attack compromises the host being remotely controlled, not only the Dameware instance. The record says authentication is required, but the CVSS vector shows only low-level privileges are needed—any authenticated Dameware user may qualify. The attack travels over the network with low complexity and no further interaction. Our reading is that the combination of network reach, low authentication bar, and control of a third host makes this worth acting on promptly, even without a CISA listing.

## What the vendor's advisory says

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

- The same release also fixes CVE-2026-28335 (buffer overflow leading to remote code execution, 8.4 High, authentication required) and CVE-2026-28327 (DLL hijacking, 8.2 High, local access with admin rights during installation only).
- The release also addresses two third-party components: CVE-2026-111497 in the Brotli decoder (buffer overflow, 9.8 Critical, unauthenticated) and CVE-2026-40021 in Apache Log4net (null byte handling, 6.3 Medium, can suppress log records).
- The release notes say DRS 12.2.4 and later require backing up registry settings and saved hosts before the first launch after upgrading; check the SolarWinds upgrade guides before starting.

## Things people will get wrong

- Authentication is required, so only an insider or compromised account poses a risk. The CVSS vector shows only low-level privileges are needed. Any user who can log in to Dameware may qualify, not only an administrator.
- It is not on CISA's exploited list, so it can wait for the next scheduled patch. The vendor scored it 9.9 Critical with a network vector and low complexity. The fix was available on 3 November 2026. Waiting for a CISA listing before acting adds unnecessary exposure.

## How we would triage it

This is our judgement.

## Step 1: Find the version of Dameware installed

- On each Windows host that may run Dameware, check the system's installed programs list and search for Dameware. Note the version number shown before making any changes.
- If Dameware Remote Support is in use, the version also appears in the DRS console under Help, then About. Record it before making any changes.

## Step 2: Restrict access to Dameware while the upgrade is arranged

- Block external access to the Dameware port at the firewall until the upgrade is confirmed. The vendor's advisory says the attack travels over the network with low complexity.
- Limit which accounts can connect to Dameware to the minimum needed. The flaw requires authentication but the CVSS vector shows only low-level privileges are sufficient.

## Step 3: Upgrade to SolarWinds Dameware 2026.3.1

- The vendor's advisory says 2026.3.1 is the fixed release, published 3 November 2026. Download it from the SolarWinds customer portal and apply it to every host running Dameware.
- The release notes say DRS 12.2.4 and later require backing up registry settings and saved hosts before the first launch after upgrade. Confirm this applies to your version before starting.

## Step 4: Confirm the upgrade and review access controls

- After upgrading, verify the installed version shows 2026.3.1 using the same check as step 1.
- Review which accounts have Dameware access and remove any that are no longer needed, reducing the low-privilege-user exposure the CVSS vector describes.

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 identified a critical vulnerability in SolarWinds Dameware (CVE-2026-28336, scored 9.9 Critical). The vendor's advisory says all versions up to and including 2026.3 are affected; the fixed release is 2026.3.1, published 3 November 2026. Please confirm whether Dameware is installed in our environment, which version is running, and whether the upgrade to 2026.3.1 has been or can be applied promptly. Please also confirm whether Dameware is reachable from outside our internal network, so we can judge whether access restrictions are needed in the meantime. We would like written confirmation of the installed version and the fix by [date].*

## 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, but not including, 2026.3

## 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 name which specific Dameware component or feature triggers the injection, so it is not possible to disable only that feature as a workaround.
- The sources do not state whether both Dameware Remote Support and Dameware Mini Remote Control are affected, or only one of the two products.
- The sources do not describe any indicator of compromise that would show whether the flaw was used against a host before the upgrade was applied.
- 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 3 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", "Why it matters", "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 by any authenticated user | Medium | This week; block external access while arranging the upgrade |
| Dameware 2026.3 or earlier on the internal network, reachable by any authenticated user | Medium | This week |
| Dameware 2026.3 or earlier, access restricted to a small group of administrators | Medium | Next patch cycle, unless you can bring it forward |
| Upgrade to 2026.3.1 not yet scheduled; on a standard monthly patch cycle | Low | Consider bringing forward given the 9.9 score |
| Already running SolarWinds Dameware 2026.3.1 | None | None for this CVE |

## 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