Node2Shell Brotli Vulnerability

On 21 October 2026, Node.js publicly disclosed a critical out-of-bounds write vulnerability in the Brotli decoder, known as Node2Shell or Brotli2Shell (CVE-2026-111497), and released fixed versions. The flaw is located in Google's open-source Brotli compression library, which is bundled in Node.js, .NET and many other runtimes and libraries. A crafted Brotli data stream can cause memory corruption, which may lead to a crash, disclosure of process memory or remote code execution. Public proof-of-concept exploits are available, and the vulnerability was added to the CISA Known Exploited Vulnerabilities catalog on 27 October 2026.

Based on the completed technical assessments, the dormakaba system solutions listed in this advisory use affected components. The actual exposure and required customer action depend on the individual product configuration and are described below.

For dormakaba-hosted cloud services, dormakaba applies the fixes. No customer action is required.

dormakaba Connector One Gen. 2 and the on-premises versions of Ambiance and Community are operated by the customer and require the customer to install updates. See Section Mitigations for details.

Customers operating separate Node.js-based applications or other software that decompresses Brotli data should assess and update those environments in accordance with the applicable vendor guidance.

Advisory Information

ID:	DKSA-26-10-111	
CVE Numbers and Scores:	CVE-2026-111497	9.2 (Critical)
Published:	10 November 2026	
Advisory Version:	1	

Affected Products

- dormakaba resivo
- dormakaba exivo

- skyra API
- Oracode
- Lyazon
- Insights API
- dormakaba Connector One Gen. 2
- Ambiance
- Ambiance Cloud
- Community
- SIMAT

Mitigations

For dormakaba-hosted cloud services, dormakaba applies the required fixes. No customer action is required.

For dormakaba Connector One Gen. 2, ensure that the product is installed in accordance with dormakaba requirements within a secure, non-public network. No immediate customer action is required when these deployment requirements are met. dormakaba will provide a fix with version 3.2.0.

The on-premises version of Ambiance is fixed in release 2.16.0, which is available for download. Customers should install this release as soon as possible.

The on-premises version of Community will be fixed in version 2.6.1 planned for 12 November 2026. Customers should install this release as soon as it becomes available.

Customers operating separate Node.js-based applications or infrastructure should update Node.js to version 22.23.4, 24.22.1 or 26.12.1 or later, as applicable to the respective release line. Node.js 20.x and older are end-of-life and should be migrated to a supported and patched release.

Software using Google Brotli directly should be updated to version 1.0.10, 1.1.1 or 1.2.1. Where an update is not immediately possible, Brotli decompression of untrusted input should be disabled.

Recommendation

The recommendation rating below applies to the dormakaba system solutions listed in this advisory.

Risk	Recommendation
☑ **High/Critical**	Updates should be applied as soon as possible based on organizational needs and threat model.
Medium	Within six months, based on organizational needs and threat model.
Low	During the next scheduled update cycle or within a year.
None / Info	Based on organizational needs and after appropriate testing.

Vulnerability Details

Brotli is a widely used open-source compression format and library maintained by Google. The vulnerability is located in the Brotli decoder itself and not in individual applications. Any software that decompresses attacker-controlled Brotli data with a vulnerable decoder can be affected. Node.js released fixed versions on 21 October 2026. Exploitation in the wild has been reported.

CVE-2026-111497 Out-of-Bounds Write in the Brotli Decoder

The decoder treats an invalid Brotli block switch as a temporary "needs more input" state instead of a permanent format error. A crafted Brotli stream can then cause the decoder to write past the end of its output buffer. This can lead to a crash, disclosure of process memory or remote code execution by an unauthenticated attacker if the affected component processes untrusted Brotli data.

- Classification / Type
    - CWE-252: Unchecked Return Value
    - CWE-787: Out-of-bounds Write
- CVSS Vector:
- CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 9.2 (Critical)
- Affected Versions:
    - dormakaba Connector One Gen. 2: All versions up to and including 3.1.1.
    - Ambiance: All versions earlier than 2.16.0.
    - Community: All versions up to and including 2.6.0.

Mitigation Details

- dormakaba resivo:

  All internet-facing resivo cloud services have been updated to the vendor-fixed Node.js release 24.22.1. One supporting function that is not directly reachable from the internet is being updated in the current development cycle. The resivo mobile apps are not affected, as they do not run Node.js on the device. No customer action is required.

- dormakaba exivo:

  The decoder was only reachable through an intra-service communication, not through externally supplied data. The upgrade to a fixed Node.js release has been implemented. No customer action is required.

- skyra API:

  The Node.js runtime used by the skyra cloud services has been updated to the vendor-fixed release. No customer action is required.

- Oracode:

The Node.js runtime used in the Oracode cloud functions has been updated to a fixed Node.js release. No customer action is required.

- Lyazon:

  The cloud functions were updated by the platform provider to the vendor-fixed Node.js runtime. No customer action is required.

- Insights API

  The Node.js runtime of the Insights API is managed by the cloud provider and has been updated to the vendor-fixed release. No customer action is required.

- dormakaba Connector One Gen. 2

  The affected function is only reachable through the configuration web page, which has to be activated locally by pressing a button on the device and is deactivated again afterwards. When the product is installed in compliance with dormakaba's requirements, in a secure, non-public environment, there is no impact. The Node.js version will be updated with firmware version 3.2.0. No customer action is required until then.

- Ambiance

  The on-premises version of Ambiance is fixed in release 2.16.0, which is available for download. Customers should install this release as soon as possible.

- Ambiance Cloud

  The .NET Runtime of Ambiance Cloud is managed by dormakaba and is planned to be updated on 18 November 2026. No customer action is required.

- Community

  The on-premises version of Community will be fixed in version 2.6.1 planned for 12 November 2026. Customers should install this release as soon as it becomes available.

- SIMAT

  The .NET Runtime of SIMAT is planned to be updated on 12 November 2026. No customer action is required.

Additional Information

Legal Disclaimer

Please ensure that your security measures comply with relevant regulatory requirements, including privacy and notification obligations.

Terms of Use

This content is licensed under the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/). If you distribute this content, or a modified version of it, you must provide attribution to dormakaba and provide a link to the original.

Additional Resources

- https://dormakabagroup.com/en/security
- product.security@dormakaba.com

Appendix

CVSS Scoring

Vulnerability classification has been performed using the CVSS v4.0 scoring system. The base score should be supplemented with an analysis of the affected environment (i.e., Environmental Metrics).

The CVSS scores defined in this advisory are intended to measure the severity of specific vulnerabilities and should not be used alone to assess risk.

Severity	A qualitative measure of a vulnerability within the scope of a specific system.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST SP 800-30).

Estimated Risk Scores

dormakaba qualifies identified vulnerabilities using the OWASP Risk Rating Matrix, assessing likelihood and impact to ensure a consistent, transparent, and business-relevant severity classification based on the system's standard configuration and a "typical" user's environment. This approach supports dormakaba's responsible disclosure process by communicating an estimated risk and remediation prioritization to stakeholders.