TLP:CLEAR【全分野】

別紙

2026 年 10 月 28 日

内閣官房　国家サイバー統括室
対処調整・官民連携等ユニット

Google Brotli ライブラリおよびそれを利用する製品の深刻な脆弱性 (CVE-2026-111497)について(注意喚起)

1. 対象ソフトウェア

データ圧縮ライブラリである Google Brotli の以下のバージョンが本脆弱性の影響を受けます。

- 1.0.3 以上 1.0.10 未満
- 1.1.0 以上 1.1.1 未満
- 1.2.0 以上 1.2.1 未満

また、本脆弱性は Google Brotli ライブラリに起因するため、Node.js、Bun、Envoy Proxy、Istio、Microsoft .NET をはじめ、Google Brotli を内部で利用している製品やソフトウェアも影響を受ける可能性があります（参考 URL①）。利用中の製品については、各ベンダーが提供するアドバイザリを確認してください。なお、本脆弱性は「Node2Shell」や「HTTP2Shell」といった名称で言及されることがあります。

2. 脆弱性悪用による影響等

対象製品には境界外書き込みの脆弱性が存在し、認証されていないリモートの攻撃者が細工された圧縮データを処理させることで、メモリ破損、プロセス異常終了、プロセス内メモリの情報漏えい、さらには任意コードの実行が発生する可能性があります。

3. 悪用状況

CVE-2026-111497 は、CISA が提供する KEV カタログに追加されており、実際に悪用されていることが確認されています（参考 URL②）。

4. 対応

開発元が提供する情報に基づき、脆弱性が修正されたバージョンにアップデートするとともに、侵害の有無を確認することを強く推奨します（参考 URL①、③）。

参考 URL

① OpenAI, Brotli decoder vulnerability
https://patchtheplanet.org/brotli

② CISA, CISA Adds Two Known Exploited Vulnerabilities to Catalog (2026/10/27)
https://www.cisa.gov/news-events/alerts/2026/10/27/cisa-adds-two-known-exploited-vulnerabilities-catalog

③ GitHub, google/brotli Release list
https://github.com/google/brotli/releases