



# Crypt::SecretBuffer versions before 0.019 for Perl is suseceptible to timing attacks

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-5086
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 23:16:27 UTC
<b>Updated</b>	2026-04-14 02:16:05 UTC
<b>Description</b>	Crypt::SecretBuffer versions before 0.019 for Perl is suseceptible to timing attacks. For example, if Crypt::SecretBuffer was

## Risk And Classification

**Problem Types:** CWE-208 | CWE-208 CWE-208 Observable Timing Discrepancy

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NERDVANA	CryptSecretBuffer	affected 0.019 custom	Not specified

## References

Reference	Source	Link
<a href="http://www.openwall.com/lists/oss-security/2026/04/13/12">www.openwall.com/lists/oss-security/2026/04/13/12</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.c</a>
<a href="https://metacpan.org/release/NERDVANA/Crypt-SecretBuffer-0.019/source/Changes">metacpan.org/release/NERDVANA/Crypt-SecretBuffer-0.019/source/Changes</a>	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://metacpan.org">metacpan.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

### Solutions

**CNA:** Upgrade to version 0.019 or later.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)