An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605130240

# NCSC Advisory

## Exim: Remote Code Execution via BDAT Use-after-free

## CVE-2026-45185

**13 May 2026**

**STATUS: TLP:CLEAR**

**Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

**For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.**

# Description

CVE ID: CVE-2026-45185

**Published:** 2026-05-12

**Vendor:** Exim

**Product:** Exim

**CVSS Score[1]:** 9.8

# Products Affected

| Product | Version |
|---|---|
| Exim | 4.97 < 4.99.3 |

# Impact

A remotely reachable memory corruption issue was discovered in Exim's GnuTLS backend. The vulnerability is triggered during BDAT message body handling when a client sends a TLS close_notify alert before the body transfer is complete, and then follows up with a final byte in cleartext on the same TCP connection.

This sequence of events can cause Exim to write into a memory buffer that has already been freed during the TLS session teardown, leading to heap corruption. An attacker only needs to be able to establish a TLS connection and use the CHUNKING (BDAT) SMTP extension.

All Exim versions from 4.97 up to and including 4.99.2 are affected. This vulnerability only impacts builds that use USE_GNUTLS=yes. Builds using OpenSSL or other TLS libraries are not affected.

Common Weakness Enumeration (CWE)[2]: CWE-416: Use After Free

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. There is no mitigation available for this vulnerability. Affected organisations should upgrade to Exim 4.99.3 as soon as possible.

- https://nvd.nist.gov/vuln/detail/CVE-2026-45185
- https://www.cve.org/CVERecord?id=CVE-2026-45185
- https://exim.org
- https://code.exim.org/exim/wiki/wiki/EximSecurity
- https://xbow.com/blog/dead-letter-cve-2026-45185-xbow-found-rce-exim
- https://news.ycombinator.com/item?id=48111748
- https://www.openwall.com/lists/oss-security/2026/05/12/4
- http://www.openwall.com/lists/oss-security/2026/05/12/25