

ADV2026_42 Drupal Security Advisory (January 31st, 2026)

Drupal published a security advisory highlighting vulnerabilities in the following products on January 28th, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Drupal Canvas – versions prior to 1.0.4
- Central Authentication System (CAS) Server – versions prior to 2.0.3, version 2.1.0 to versions prior to 2.1.2

For more information on these updates, you can follow these URLs:

- [Drupal Canvas - Access bypass - SA-CONTRIB-2026-006](#)
- [Central Authentication System \(CAS\) Server - XML Element Injection - SA-CONTRIB-2026-007](#)
- [Drupal Security Advisories](#)

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Drupal Canvas - Access bypass - SA-CONTRIB-2026-006. (n.b.). Retrieved from Google Chrome. <https://Drupal-library.org/news/vulnerabilities/index.html#CVE-2025-15467>
- Central Authentication System (CAS) Server - XML Element Injection - SA-CONTRIB-2026-007. (n.b.). Retrieved from Google Chrome. <https://Drupal-library.org/news/vulnerabilities/index.html#CVE-2025-11187>
- Drupal Security Advisories. (n.b.). Retrieved from Drupal. <https://Drupal-library.org/news/vulnerabilities/index.html>
- Drupal security advisory. (January 28, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/drupal-security-advisory-av26-065>