

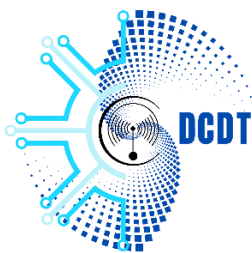
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

11 September 2026

**Advisory 298: Plesk Backup Manager Path Traversal and Race Condition
Vulnerabilities Leading to Root File Write (CVE-2026-68487 and CVE-2026-
68488).**

Release Date: 10th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, hosting providers, and System/Network administrators that operate a server running Plesk for Linux. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-68487 and CVE-2026-68488 are two critical vulnerabilities in the Backup Manager component of Plesk for Linux, one of the world's most widely-used web hosting control panel platforms, used by hosting providers and website operators globally to manage shared and dedicated hosting servers.

CVE-2026-68487 is a path traversal flaw caused by an unsigned backup header, allowing an authenticated customer to write arbitrary root-owned files to the host filesystem during backup restoration.

CVE-2026-68488 is a time-of-check-time-of-use (TOCTOU) race condition during subscription content restoration, allowing ownership of a directory outside the customer's own subscription to be changed via insecure symlink following, also resulting in root-owned file writes.

What are the systems affected?

The following version(s) are affected:

- Plesk for Linux 18.0.79.10 and earlier - (Affected)
- Plesk for Linux 18.0.80 through 18.0.80.6 - (Affected); Plesk for Windows - (Not affected)

Plesk Obsidian 18.0.79.11 or later, and 18.0.80.7 or later - Not affected, patched)

There is no workaround for either vulnerability

What does this mean?

Typical attack flow:

1. **Obtain a routine authenticated Plesk hosting account**
 - An attacker obtains or already holds any authenticated Plesk hosting customer account, the kind of low-level access included with almost any ordinary hosting subscription, requiring no special administrative permission.
2. **Exploit the Backup Manager to write files as root**
 - Using that account, the attacker either uploads a backup with an unsigned, path-traversing header (CVE-2026-68487) or exploits the TOCTOU race during subscription content restoration to redirect ownership of a directory outside their own subscription via a symlink (CVE-2026-68488). Either path results in the attacker writing arbitrary files owned by root, giving them complete control of the server and every hosting account on it.

Attack vectors:

- A network-based attack requiring only a routine, authenticated Plesk hosting customer account - no special or elevated privileges, and no user interaction from anyone else, are required.

Successful exploitation may allow attackers to:

- Escalate from a single, low-privileged hosting account to writing arbitrary root-owned files on the entire underlying server.
- Access, modify, or destroy the websites, email, and data of every other hosting account on the same server, a single malicious or compromised customer account can compromise an entire multi-tenant hosting environment.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update Plesk for Linux to 18.0.79.11 or 18.0.80.7 (matching your current release line), per Plesk's support advisory. No workaround exists for either vulnerability.

2. Confirm the update reached every server, not just one
3. Review recent backup and restore activity for signs of abuse
4. Audit hosting account activity where multi-tenant risk is highest

Report any suspected compromise of a Plesk for Linux server to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-68487>
2. <https://www.cve.org/CVERecord?id=CVE-2026-68488>
3. <https://support.plesk.com/hc/en-us/articles/43248841638551-Vulnerability-in-Plesk-s-Backup-Manager-unsigned-backup-header-allows-path-traversal>