SA No.: SA-2026-02
Notification Date: October 30, 2026

SECURITY ADVISORY

PHP2Shell Vulnerabilities in WebAccess/VPN

Summary

Two critical PHP vulnerabilities, CVE-2026-109618 and CVE-2026-109619, can allow an unauthenticated remote attacker to execute code on a WebAccess/VPN server. All versions of WebAccess/VPN on Ubuntu 20.04, 22.04, 24.04, and 26.04 are affected. Install the PHP2Shell security patch on every affected server as soon as possible.

Issue Description

PHP2Shell comprises two memory-safety flaws in PHP request handling. WebAccess/VPN runs its web interface on PHP under Apache `mod_php`. In this configuration, an attack can succeed before application code runs, so the WebAccess/VPN login does not protect against it. Exploitation depends on memory layout and timing; working attacks are in use.

- **CVE-2026-109618:** PHP can run out of memory while setting up a request and later use partially initialized request data.
- **CVE-2026-109619:** Request state can outlive the memory it refers to, allowing a later request handled by the same worker to use freed memory.

Severity

- CVE-2026-109618: CVSS 4.0 Base Score 9.2 (Critical)
- CVE-2026-109619: CVSS 4.0 Base Score 9.2 (Critical)

Affected Products

All versions of WebAccess/VPN (VPN Portal) running on Ubuntu 20.04, 22.04, 24.04, or 26.04 are affected. A server remains vulnerable until the PHP2Shell patch is installed.

Long-Term Platform Recommendation

WebAccess/VPN uses PHP 5.6, which reached end of life on 31 December 2018. The PHP2Shell patch fixes only the two CVEs in this advisory; it does not restore upstream PHP support or address other issues in the legacy platform. Plan a long-term migration from WebAccess/VPN (VPN Portal) to WebAccess/DMP; confirm device compatibility and migration requirements with Advantech.

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic
Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz
IČO: 24148661
DIČ: CZ24148661

Solution

The offline package `vpnportal-php2shell-offline.tar.gz` installs a build of the PHP version used by WebAccess/VPN with fixes for both CVEs. Apply it on every WebAccess/VPN server as soon as possible. Download the package: vpnportal-php2shell-offline.tar.gz. Direct URL: `https://sendfiles.advantech.cz/custom-download.php?link=vpnportal-php2shell-offline.tar.gz`

1. Verify that `sha256sum vpnportal-php2shell-offline.tar.gz` prints this SHA-256 value:

   ```
   5e692fb2790626eb995c272c62a4495062be72eec5d01d11b33200d22b284972
   ```

2. Copy the package to the server and unpack it with `tar -xzf vpnportal-php2shell-offline.tar.gz`.
3. Apply the patch by running `sudo bash vpnportal-php2shell-offline/vpnportal-php2shell-patch.sh`.
4. Confirm that the last output line reads `RESULT: PHP2Shell patch applied successfully`.

The package applies to any WebAccess/VPN version on Ubuntu 20.04, 22.04, 24.04, and 26.04. On Ubuntu 20.04 the PHP version number may decrease; this is expected because the new build includes all security fixes up to and including PHP2Shell.

Applying the patch restarts Apache. The web interface may be unavailable for a few seconds, but VPN connections are not interrupted. The patch is safe to run more than once. If it stops with an error, send `/var/log/vpnportal-php2shell.log` to Regional Support.

Access Restriction

Restrict HTTPS access to WebAccess/VPN (VPN Portal) to trusted IP addresses or networks with a firewall. Where feasible, expose it only through a separate VPN. Keep this restriction until the portal is migrated or decommissioned. This reduces exposure but does not replace the PHP2Shell patch.

Related Advisories

CVE-2026-109618, CVE-2026-109619

References

- PHP project: CVE-2026-109618 security advisory
- PHP project: CVE-2026-109619 security advisory
- watchTowr: CVE-2026-109618 FAQ
- Qualys: PHP security release for two vulnerabilities
- PHP project: unsupported PHP branches (PHP 5.6 end of life)
- Advantech: WebAccess/DMP Device Management Platform

Revision History

2026-10-30 Advisory published; long-term platform recommendations added

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661