BEZPEČNOSTNÍ UPOZORNĚNÍ

Kritické zranitelnosti PHP v MyQ

Doporučení pro MyQ Print Server a MyQ Central Server

Podstatné: MyQ 10.2 LTS Patch 29 obsahuje opravenou verzi PHP. Doporučujeme aktualizaci provést co nejdříve.

O co jde

Dne 21. 10. 2026 byly zveřejněny opravy dvou kritických zranitelností PHP: CVE-2026-109618 a CVE-2026-109619 (CVSS 9.0 a 9.2). Za určitých podmínek mohou umožnit neautentizovanému útočníkovi vzdálené spuštění kódu na zasaženém serveru.

Podle oznámení MyQ jsou dotčeny MyQ Print Server a MyQ Central Server, které obsahovaly PHP bez těchto oprav. MyQ Roger není dotčen, protože PHP nepoužívá.

Kterých verzí se problém týká

Verze MyQ	Stav	Řešení
MyQ 10.2 LTS (do Patch 28)	Dotčeno PHP 8.3.35	Aktualizovat na MyQ 10.2 LTS Patch 29 (PHP 8.3.36).
MyQ 10.3.0	V době oznámení ještě nebyla vydána	Má obsahovat opravenou verzi PHP již od prvního vydání.
MyQ 8.2 a jiné verze po konci životnosti	Dotčeno	Oprava pro tyto verze nebude vydána. Doporučen je přechod na MyQ 10.2 LTS Patch 29.

Doporučený postup

1. Aktualizujte MyQ Print Server a MyQ Central Server na MyQ 10.2 LTS Patch 29. Jde o řešení doporučené výrobcem.

2. Pokud aktualizaci nelze provést ihned, dočasně omezte riziko těmito opatřeními:

01	Omezit dostupnost serveru Server MyQ by neměl být přímo dostupný z internetu.
02	Omezit přístup v síti Povolit přístup jen sítím, uživatelům a zařízením, které jej potřebují.
03	Kontrolovat logy Sledovat neobvyklou aktivitu, zejména neočekávané procesy spouštěné pomocí php-cgi.exe.

AKTUALIZACE VYDÁNA	MyQ oznámilo vydání MyQ Central Server 10.2 (Patch 29) a MyQ Print Server 10.2 (Patch 29).

Informace vychází z bezpečnostního oznámení MyQ Security Announcements. Před aktualizací ověřte konkrétní verzi a postup pro vaše prostředí.