

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in HP Poly PrivateConnect
Tracking #:432319350
Date:28-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HP has disclosed a critical security vulnerability affecting Poly PrivateConnect deployments that use Pexip.

TECHNICAL DETAILS:

HP has disclosed a critical security vulnerability affecting Poly PrivateConnect deployments that use Pexip. The vulnerability could allow an unauthenticated remote attacker to execute arbitrary code on affected systems, potentially leading to full system compromise.

Vulnerability Details

- **CVE:** CVE-2026-TBD
- **Severity:** Critical | **CVSS:** 9.8
- A critical vulnerability in Poly PrivateConnect using Pexip may allow an unauthenticated remote attacker to execute arbitrary code remotely. Successful exploitation could result in complete system compromise, including unauthorized code execution and impacts to the confidentiality, integrity, and availability of the affected system.

Affected products	
Product Name	Updated version
Poly PrivateConnect	v38.2 v39.2 v40.1 v41

RECOMMENDATIONS:

- Immediately upgrade affected Poly PrivateConnect systems to the latest supported version.
- Prioritize remediation for internet-facing or externally accessible deployments.
- Restrict administrative access to trusted networks and authorized users.
- Monitor system and application logs for unusual activity or unauthorized access attempts.
- Follow HP and Pexip security advisories for future updates and additional guidance.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hp.com/us-en/document/ish_15324250-15324288-16/hpsbpy04135