

Ransomware Groups Exploit Patched PAN-OS and Prisma Access Flaw CVE-2026-0257



Palo Alto Networks reports continued ransomware exploitation of CVE-2026-0257, an authentication bypass in PAN-OS and Prisma Access that allows unauthorized VPN connections. A patch has been available since May 2026.

- CVE-2026-0257 is an authentication bypass in PAN-OS and Prisma Access, rated CVSS 7.8.
- It can be used to set up unauthorized VPN connections.
- Palo Alto Networks patched it in May 2026 but still sees exploitation by ransomware actors.
- The headline names the Qilin and INC ransomware groups as exploiting it to bypass MFA.

What was reported

Palo Alto Networks has said it continues to see ransomware actors exploiting CVE-2026-0257, a flaw affecting PAN-OS and Prisma Access. The issue is an authentication bypass, scored 7.8 on the CVSS scale, that attackers can use to establish VPN connections without authorization.

The vendor released a fix in May 2026. According to the report's headline, the Qilin and INC ransomware groups are among those using the flaw to get around multi-factor authentication.

Why it matters

Remote-access gateways are a common entry point for ransomware operations. A bypass of authentication on a VPN service means that MFA, which many institutions rely on as a key control, may not protect an unpatched gateway. Exploitation continuing months after the patch suggests that some devices remain unpatched.

The source excerpt does not give details on affected versions, victims or indicators of compromise, so teams should consult the vendor's advisory for those specifics.

What to do next

Treat this as a patching and verification task rather than an emergency redesign. Confirm that every PAN-OS and Prisma Access instance, including those managed by third parties, runs a fixed release, and review VPN logs for unexpected sessions.

What to do now

1. Inventory all PAN-OS and Prisma Access instances, including those run by service providers.
2. Apply the May 2026 fix for CVE-2026-0257 per Palo Alto Networks' advisory.
3. Review VPN logs for unauthorized or unusual connections, especially from before patching.
4. Do not rely on MFA alone for remote access; add monitoring of gateway sessions.
5. Confirm patch status with managed-service providers and record it for NCA ECC and SAMA CSF evidence.