

Fortra Patches Critical Vulnerabilities in Core Privileged Access Manager (CVE-2026-79901, CVE-2026-79898, CVE-2026-12627, and more)

Oct 05, 2026

☐ WHITE

[View Alert](#)

Fortra has [released](#) software updates to address eight security flaws in its **Core Privileged Access Manager (BoKS)** software, which provides centralized account management and policy enforcement for Unix and Linux systems. Three of the eight vulnerabilities were deemed critical and tracked as [CVE-2026-79901](#), [CVE-2026-79898](#), and [CVE-2026-12627](#).

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerabilities.

Additional Info

Analysis

On October 01, 2026, Fortra [released](#) software updates addressing [eight vulnerabilities](#) in its **Core Privileged Access Manager (BoKS)** tool, which centralizes account management and access enforcement across Unix and Linux operating systems. The patch set resolves three primary flaws:

- An authentication bypass involving predictable Active Directory password generation.
- A command injection flaw within the crlserver component.

- A stack buffer overflow that affects the autoregistration feature.

Below are the eight vulnerabilities patched by Fortra:

- [CVE-2026-79901](#) (CVSS: 9.9 / Critical) - An authentication bypass flaw in BoKS Manager keytab-based Active Directory service account management caused by predictable pseudo-random password generation seeded using timestamps, permitting offline candidate verification.
- [CVE-2026-12627](#) (CVSS: 9.8 / Critical) - A stack-based buffer overflow vulnerability in BoKS's autoregistration functionality (boks_autoregisterd) that allows remote attackers to trigger memory corruption.
- [CVE-2026-79898](#) (CVSS: 9.1 / Critical) - An OS command injection flaw in crlserver that permits an authenticated user via BCC, WSI APIs, or CLI interfaces to substitute shell commands processed as root on the BoKS Master.
- [CVE-2026-14316](#) (CVSS: 8.1 / High) - A heap-based buffer overflow vulnerability (CWE-122) exists in Fortra's boks_sshd revoked-key error handling.
- [CVE-2026-79899](#) (CVSS: 7.9 / High) - An insecure temporary file vulnerability in the bccgethostcert utility due to missing a restrictive umask, allowing local users with access to BOKS_tmp to view sensitive cryptographic material.
- [CVE-2026-79896](#) (CVSS: 7.5 / High) - An out-of-bounds read vulnerability in the custom TLS ClientHello component (boks_portmux).
- [CVE-2026-79900](#) (CVSS: 6.5 / Medium) - A heap overflow vulnerability in Fortra boks_ksllogsd due to improper bounds checking of checksum algorithm names supplied in authenticated KSL start messages, allowing an authenticated client to write beyond the end of a heap allocation.
- [CVE-2026-9864](#) (CVSS: 4.8 / Medium) - A predictable password generation vulnerability in the adjoin utility, where machine-account passwords generated during Active Directory join or password renewal operations have lower entropy than intended and are susceptible to prediction.

In the health sector, hospitals and medical facilities rely heavily on Linux and Unix environments to run core electronic health record platforms, laboratory information systems, and medical device gateways. Privileged access software manages administrative rights across these critical servers. An

intruder gaining access via these vulnerabilities could compromise master directory credentials, manipulate medical data pipelines, or disrupt clinical workflows essential to patient care.

Securing these administrative access channels is vital for protecting sensitive patient data and maintaining compliance with healthcare privacy regulations. Health sector organizations frequently utilize automated systems and integrated directory services to streamline staff access, making flaws in directory synchronization and privilege management particularly significant risks for hospital networks. Implementing rapid vendor patches helps safeguard medical infrastructure against unauthorized operational disruptions.

Recommendations

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and implement the following:

- [Apply](#) the latest software updates provided by Fortra for the Core Privileged Access Manager (BoKS) across all administrative servers.
- Audit Active Directory service account configurations and keytab management practices to prevent predictable password generation issues.
- Restrict network access to management interfaces, APIs, and components such as crlserver using internal network segmentation.
- Monitor privileged session logs and account authentication events for anomalous command execution patterns or unauthorized access attempts.
- **Reviewing the Health Industry Cybersecurity Practices (HICP):** [Managing Threats and Protecting Patients Resources](#).

Alert Id	a301dae4
Category	Vulnerability Bulletins
References	fortra fortra 1 fortra 2 fortra 3 fortra 4 fortra 5 fortra 6 hhs fortra 7 securityweek fortra 8

Tags

CVE-2026-79900, CVE-2026-79899, CVE-2026-79896, CVE-2026-9864, CVE-2026-14316, CVE-2026-12627, CVE-2026-79898, CVE-2026-79901, Fortra Core Privileged Access Manager, Fortra BoKS, Fortra

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback



Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org

--

You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.

To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.

To view this discussion visit <https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a10a0db8ef-ab6490b8-3c9a-4ac8-86a7-3f14ee69253b-000000%40email.amazonses.com>.