Delinea

Security Advisories

This page provides timely updates on software vulnerabilities, patches, and security-related issues that may impact our products or services. We're committed to transparency and proactive communication to help you stay informed and protected.

Check back regularly for the latest advisories, mitigation guidance, and best practices to ensure your systems remain secure.

- Authentication Bypass via SAML Response Manipulation - CVE-2026-15640
- Reflected Cross-Site Scripting - CVE-2026-15639
- Cryptographic Padding Oracle - CVE-2026-15638
- Delinea Secret Server on-prem FIDO2 credential registration authentication bypass vulnerability - CVE-2026-19117
- Delinea Cloud Suite on-prem argument injection vulnerability - CVE-2026-2409
- Delinea Cloud Suite and Privileged Access Service – SQL Injection vulnerability - CVE-2025-12812
- Delinea Cloud Suite and Privileged Access Service – HTTP Request Smuggling vulnerability - CVE-2025-12811
- Delinea Secret Server on-prem RPC Password Rotation authentication vulnerability - CVE-2025-12810
- Delinea Secret Server on-prem SQL report creation vulnerability - CVE-2025-6943
- Delinea Secret Server on-prem distributed engine authentication process vulnerability - CVE-2025-6942

Delinea makes no warranties of any kind, whether express, implied, statutory, or otherwise, and specifically, disclaims all warranties of fitness for a particular purpose, merchantability, accuracy of informational content, systems integration, non-infringement, non-interference with enjoyment or otherwise. Under no circumstances shall Delinea be liable for any damages whatsoever including direct, indirect, special, punitive or consequential loss or damage, including loss of profits, loss of business, loss of revenue, loss of or damage to goodwill, or loss of data. The foregoing exclusions will not apply to the extent prohibited by applicable law.

Delinea

© 2026 Copyright Delinea

Privacy Policy | Terms of Use | MSLA | Sitemap | Your Privacy Choices