GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

3 September 2026

Advisory 244: Delinea Secret Server (On-Prem) FIDO2 Authentication Bypass (CVE-2026-19117).

Release Date: 2nd September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and Identity/Privileged Access Management (PAM) teams that deploy or operate Delinea Secret Server as an on-premises secrets vault. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-19117 is a critical authentication-bypass vulnerability in on-premises deployments of Delinea Secret Server, a widely-used Privileged Access Management (PAM) and secrets-management platform that organizations rely on to centrally store, control, and audit access to administrative passwords, API keys, certificates, and other sensitive credentials. Under specific conditions, an attacker can register an attacker-controlled FIDO2 (hardware security key/passwordless) credential against a target user account, and then use that attacker-controlled credential to authenticate as that user - bypassing the account's intended authentication controls entirely.

What are the systems affected?

The following version(s) are affected:

- Delinea Secret Server (On-Prem) 10.6.0, 11.8.0, 11.9.0, and 12.0.0 branches, up to and including the last build prior to each branch's fix – (Affected)

Delinea Secret Server (On-Prem) 12.1.000003 and later on the 12.1.x branch – (Not affected, patched). Delinea's own release notes confirm the fix landed in 12.1.000003; CERTVU could not independently confirm the specific fixed build number for the 10.6.x, 11.8.x, 11.9.x, or 12.0.x branches from public sources and recommends organizations on an older branch contact Delinea support directly to confirm the correct fixed build, or upgrade to the current 12.1.x release. Secret Server Cloud (SaaS) deployments are not affected by this CVE.

What does this mean?

Typical attack flow:

1. **Register an attacker-controlled FIDO2 credential against a target account**
    - Under specific conditions, an attacker registers a FIDO2 (hardware security key/passwordless) credential that they control against a target user account on a reachable, unpatched Secret Server (On-Prem) instance.
2. **Authenticate as the target user**
    - The attacker then uses the attacker-controlled FIDO2 credential to authenticate as the target user, bypassing that account's intended authentication controls and gaining access to every secret, credential, and privileged system access the compromised account is entitled to.

Attack vectors:

- A network-based request against any internet- or network-reachable Secret Server (On-Prem) instance running an affected version.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation but the technical details are now public and the maximum-possible impact of a successful compromise (full access to a privileged-credential vault) warrants urgent action.

Successful exploitation may allow attackers to:

- Authenticate as a privileged Secret Server user without ever presenting a legitimate credential, undermining the authentication boundary the platform exists to enforce.
- Access, exfiltrate, or modify every secret, credential, API key, and certificate the compromised account is entitled to view within Secret Server, and use those harvested credentials to pivot into every downstream system, application, or infrastructure component that the vault was protecting.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor fix without delay

- Upgrade Secret Server (On-Prem) to 12.1.000003 or later. If running an older branch (10.6.x, 11.8.x, 11.9.x, or 12.0.x), contact Delinea support to confirm the correct fixed build for that branch, or plan an upgrade to the current 12.1.x release.

2. Review and audit all FIDO2/security-key credentials registered in Secret Server, since this is the specific mechanism this vulnerability abuses
3. Audit the estate for Secret Server deployments
4. Treat any internet-reachable, unpatched instance as potentially compromised
5. Rotate secrets and credentials

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-19117
2. https://delinea.com/security-advisories