مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Delinea Secret Server

Tracking #:432315763

Date:16-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Delinea patches an API vulnerability in Secret Server Cloud and Secret Server On-Premises.

TECHNICAL DETAILS:

Delinea Secret Server (formerly Thycotic Secret Server) is a privileged access management (PAM) solution "for the modern, hybrid enterprise".

Affected Product: Delinea Secret Server (on-premises installations)
Vulnerability: Authentication bypass in the SOAP API
Severity: Critical
Exploit: Available
Impact: Attackers could gain full administrative access and steal stored secrets.

Fixed Versions:

- Delinea Platform and Secret Server Cloud have been patched and are no longer vulnerable.
- For Versions 11.5.000002 and later upgrade to Secret Server On-Premises Version 11.7.000001

Mitigations:

- Versions prior to 11.5.000002-On the Secret Server application server, edit the web.config file located at C:\inetpub\wwwroot\SecretServer\webservices\web.config.
- To properly modify the web.config file in the webservices directory, find the <configuration> element and update the elements below to block all access to the affected web service endpoints. After saving this file, the settings will take effect immediately.

RECOMMENDATIONS:

- Update immediately: Update to the latest patched version for on-premises installation, as soon as possible.
- Disabling SOAP endpoints for Secret Server Cloud customers until a patch was deployed.
- Check for suspicious activity: Investigate audit logs for any unauthorized access attempts

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.delinea.com/s/article/KB-010572-How-do-I-remediate-Secret-Server-in-reference-to-the-Secret-Server-SOAP-vulnerability