مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Forcepoint One DLP Client

Tracking #:432318218

Date:07-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Forcepoint One Data Loss Prevention (DLP) Client that may allow attackers to bypass sandbox restrictions and execute arbitrary code on protected endpoints.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in the Forcepoint One Data Loss Prevention (DLP) Client that may allow attackers to bypass sandbox restrictions and execute arbitrary code on protected endpoints. Exploitation of this flaw could weaken DLP enforcement and reduce overall endpoint security.

Vulnerability Details

- **CVE-2025-14026**
- CVSS Score: 7.8 High
- The Forcepoint One DLP Client shipped a legacy Python 2.5.4 runtime intended for internal use. To prevent misuse, the ctypes library was removed to restrict access to system-level functions. However, this limitation can be bypassed by transferring the missing ctypes module and applying a version-header patch. Once restored, the Python environment can execute arbitrary shellcode or DLL-based payloads, giving attackers full control within the client process.
- Exploitation of this vulnerability may allow attackers to bypass DLP controls, evade security monitoring, and alter endpoint client behavior.

Affected Versions:

- Forcepoint One DLP Client 23.04.5642 and potentially earlier releases containing the bundled Python runtime.

Fixed Versions

- Forcepoint One Endpoint builds v23.11 and later (Forcepoint DLP v10.2+)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Forcepoint.

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://nvd.nist.gov/vuln/detail/CVE-2025-14026