مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-CrowdStrike Falcon Sensor for Windows

Tracking #:432317793

Date:09-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed CrowdStrike has released security updates addressing two medium-severity vulnerabilities impacting the Falcon Sensor for Windows, that could allow an attacker with existing local code execution privileges to delete arbitrary files on the affected host system.

TECHNICAL DETAILS:

CrowdStrike has released security updates addressing two medium-severity vulnerabilities impacting the Falcon Sensor for Windows. These vulnerabilities — CVE-2025-42701 (Race Condition) and CVE-2025-42706 (Logic Error) — could allow an attacker with existing local code execution privileges to delete arbitrary files on the affected host system.

While exploitation requires prior access and execution rights on the host, successful exploitation could cause stability or functionality issues with the Falcon sensor, operating system, or other installed software.

CrowdStrike confirms no active exploitation in the wild. Fixes are available in Falcon Sensor for Windows version 7.29 and hotfix releases for versions 7.16, 7.24–7.28. Customers are urged to upgrade immediately.

Vulnerability Details:

1. **CVE-2025-42701**
   - Type: Time-of-check Time-of-use (TOCTOU) Race Condition
   - CWE: 367 - Race Condition
   - CAPEC: 27 - Leveraging Race Conditions via Symbolic Links
   - CVSS v3.1 Score: 5.6 (MEDIUM)
   - Impact: Permits attackers with code execution on the host to exploit a race condition, potentially deleting arbitrary files through a symbolic link attack.

2. **CVE-2025-42706**
   - Type: Logic Error in Origin Validation
   - CWE: 346 - Origin Validation Error
   - CAPEC: 473 - Signature Spoof
   - CVSS v3.1 Score: 6.5 (MEDIUM)
   - Impact: Logic flaw lets attackers with prior code execution capability delete arbitrary files.

Affected Versions:

- 7.28.20006 and earlier
- 7.27.19907
- 7.26.19811 / 7.26.19809
- 7.25.19706
- 7.24.19607 and earlier
- 7.16.18635 and earlier for Win7/2008 R2

Patched Versions:

- 7.28.20008 and later
- 7.27.19909
- 7.26.19813
- 7.25.19707
- 7.24.19608
- 7.16.18637 (Win7/2008 R2 only)

Not Impacted:

- Falcon Sensor for Mac
- Falcon Sensor for Linux
- Falcon Sensor for Legacy Windows

RECOMMENDATIONS:

- Upgrade Now: Immediately update to the latest Falcon Sensor for Windows or apply the appropriate hotfixes.

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://www.crowdstrike.com/en-us/security-advisories/issues-affecting-crowdstrike-falcon-sensor-for-windows/