Lưu ý kỹ thuật | Các issue ảnh hưởng đến Falcon Sensor dành cho Windows

Cloud: US-1 US-2 EU-1
Solution: Sensors - Windows OS Platforms

Ngày công bố: Ngày 9/10/2025

Tóm Tắt

Chúng tôi đã phát hành các bản vá cho hai issue ảnh hưởng đến Falcon Sensor cho Windows. Cả hai issue này đều có một điều kiện tiên quyết: **kẻ tấn công phải xâm nhập và đã có quyền thực thi code trên host từ trước**. Một khi đã có quyền này, chúng có thể xóa các file nhất định. Các bản vá cho cả hai issue đều có trong phiên bản Falcon Sensor cho Windows mới nhất là 7.29, trong các bản vá nóng (hotfix) cho các phiên bản từ 7.24 đến 7.28 và trong một bản vá nóng 7.16 cho các host đang chạy Windows 7/2008 R2. Bản vá nóng phiên bản 7.24 cũng sẽ được cập nhật cho Long-Term Visibility (LTV) Sensor cho Windows IoT.

Hiện không có dấu hiệu nào cho thấy các issue này đã bị khai thác trong thực tế. Các đội ngũ săn tìm mối đe dọa và tình báo của chúng tôi đang chủ động giám sát các hành vi khai thác và chúng tôi duy trì khả năng quan sát đối với bất kỳ hành vi tương tự nào như vậy.

Chúng tôi đang công khai các issue này cùng với các bản vá một cách đồng thời, tuân thủ theo các quy trình tiêu chuẩn của ngành về việc công khai lỗ hổng có phối hợp để đảm bảo khách hàng của chúng tôi luôn được bảo vệ.

Tác Động

Việc khai thác các issue này để xóa file có thể tiềm ẩn nguy cơ dẫn đến các sự cố về tính ổn định hoặc chức năng của CrowdStrike Falcon Sensor cho Windows hoặc của các phần mềm khác trên hệ thống, bao gồm cả hệ điều hành.

Falcon Sensor cho Mac, Falcon Sensor cho Linux và Falcon Sensor cho các Hệ thống Windows Cũ (Legacy) sẽ không bị ảnh hưởng.

Tổng Quan Kỹ Thuật

Tồn tại một lỗi logic trong Falcon Sensor cho Windows có thể cho phép một **kẻ tấn công đã xâm nhập và có khả năng thực thi code trên một host từ trước thực hiện xóa các file nhất định**. CrowdStrike đã phát hành một bản vá bảo mật cho issue này trong các phiên bản Falcon Sensor cho Windows từ 7.24 trở lên và tất cả các Long Term Visibility (LTV) Sensor. Những issue này đã được xác định thông qua chương trình Bug Bounty và là một phần trong hình thái bảo mật toàn diện của chúng tôi.

Các Phiên Bản Bị Ảnh Hưởng

Falcon Sensor cho Windows các phiên bản 7.28 và cũ hơn sẽ bị ảnh hưởng.

Các phiên bản Falcon sensor cho Windows bị ảnh hưởng
7.28.20006
7.27.19907
7.26.19811
7.26.19809
7.25.19706
7.24.19607 và cũ hơn
7.16.18635 và các bản dựng 7.16 cũ hơn (Chỉ dành cho WIN7/2008 R2)

Các bản vá Falcon sensor cho Windows
7.28.20008 và mới hơn
7.27.19909
7.26.19813
7.25.19707
7.24.19608
7.16.18637 (Chỉ dành cho WIN7/2008 R2)

Mức độ nghiêm trọng

CrowdStrike đã chấm điểm cho CVE-2025-42701 (Falcon Sensor for Windows Race Condition) là 5.6 (MEDIUM) theo Common Vulnerability Scoring System Phiên bản 3.1 (CVSS).

CrowdStrike đã chấm điểm cho CVE-2025-42706 (Falcon Sensor for Windows Logic Error) là 6.5 (MEDIUM) theo Common Vulnerability Scoring System Phiên bản 3.1 (CVSS).

Loại Điểm Yếu và Tác Động

- CVE-2025-42701 (https://www.cve.org/CVERecord?id=CVE-2025-42701) - CrowdStrike Falcon Sensor for Windows Race Condition
  - CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition
  - CAPEC-27: Leveraging Race Conditions via Symbolic Links
- CVE-2025-42706 (https://www.cve.org/CVERecord?id=CVE-2025-42706) - CrowdStrike Falcon Sensor for Windows Logic Error
  - CWE-346: Origin Validation Error
  - CAPEC-473: Signature Spoof

Trạng thái khai thác

CrowdStrike không phát hiện bất kỳ dấu hiệu nào về việc các issue này đã bị khai thác trong thực tế.

CrowdStrike đang chủ động giám sát các dấu hiệu lạm dụng hoặc sử dụng lỗ hổng này.

Tác động về hiệu suất

Không có tác động trực tiếp hay gián tiếp nào đến hiệu suất của Sensor và chúng tôi cũng không ghi nhận bất kỳ tác động nào trong quá trình kiểm thử.

Xác định các Host bị ảnh hưởng

Khách hàng có thể sử dụng câu truy vấn trên Github

Cách giải quyết

Khách hàng nên cập nhật các host Windows đang chạy Sensor với các phiên bản bị ảnh hưởng lên một phiên bản đã được vá lỗi.

Tài liệu bổ sung

- Details for CVE 2025-42701 - CrowdStrike Falcon Sensor for Windows Race Condition (https://www.cve.org/CVERecord?id=CVE-2025-42701)
- Details for CVE-2025-42706 - CrowdStrike Falcon Sensor for Windows Logic Error (https://www.cve.org/CVERecord?id=CVE-2025-42706)
- Security Advisory (https://www.crowdstrike.com/en-us/security-advisories/issues-affecting-crowdstrike-falcon-sensor-for-windows/)
- Falcon Customizable NG SIEM Dashboard for Assessing (https://github.com/CrowdStrike/logscale-community- content/blob/main/Dashboards-Only/CVE-2025-42701_CVE-2025-42706.yaml)
- Sensor Release Notes - Commercial Clouds (https://supportportal.crowdstrike.com/s/article/Release-Notes-Falcon-Sensor-for-Windows-7-16-18637-7-24-19608-7-25-19707-7-26-19813-7-27-19909-7-28-20008-Hotfixes)
- Sensor Release Notes - Gov Clouds (https://supportportal.crowdstrike.us/s/article/Release-Notes-Falcon-Sensor-for-Windows-7-16-18637-7-24-19608-7-25-19707-7-26-19813-7-27-19909-7-28-20008-Hotfixes)
- CrowdStrike Customer Center (https://supportportal.crowdstrike.com/)
- CrowdStrike Community (https://community.crowdstrike.com/emerging-threats-63/cve-2025-42701-cve-2025-42706-falcon-sensor-for-windows-medium-cves-issued- 3020?fid=63&tid=3020)

Các Câu Hỏi Bổ Sung

Nếu bạn có các câu hỏi khác, vui lòng liên hệ với Technical Account Manager, Sales Engineer, Account Manager hoặc CrowdStrike Support.