Falcon Security Bulletin

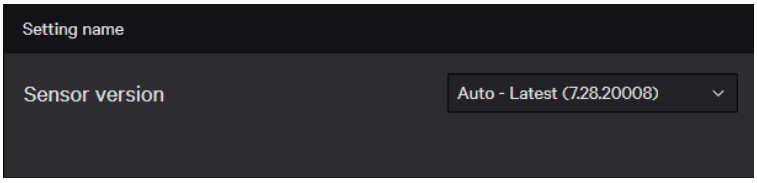
CROWDSTRIKE

MANUAL PATCH NEEDED FOR CVE-2025-42701 & CVE-2025-42706

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

SUMMARY OF UPDATE POLICY FAILURE

Following the release of fixes for recently identified vulnerabilities in CrowdStrike Falcon for Windows (**CVE-2025-42701** and **CVE-2025-42706**), the Overwatch team has identified subscriptions with a **Sensor Update Policy** using an **N-1** or an **Auto** schedule. These tenants did not include updates for the above CVEs in the v7.28 build and will need to be updated manually to the v7.29 patch in order to mitigate both vulnerabilities.



APPLY SENSOR PATCH MANUALLY

You can obtain a copy of the standalone patch tool to update Falcon for Windows manually on affected systems running versions prior to the **v7.29 release**.

Falcon Sensor Patch Tool

REVIEW SENSOR UPDATE POLICIES

Affected subscriptions will have new **Sensor Update Policy** options made available by the Overwatch team. Administrators should review their current policies and made the necessary adjustments to ensure timely patching of affected endpoints.

Falcon Console Login

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**