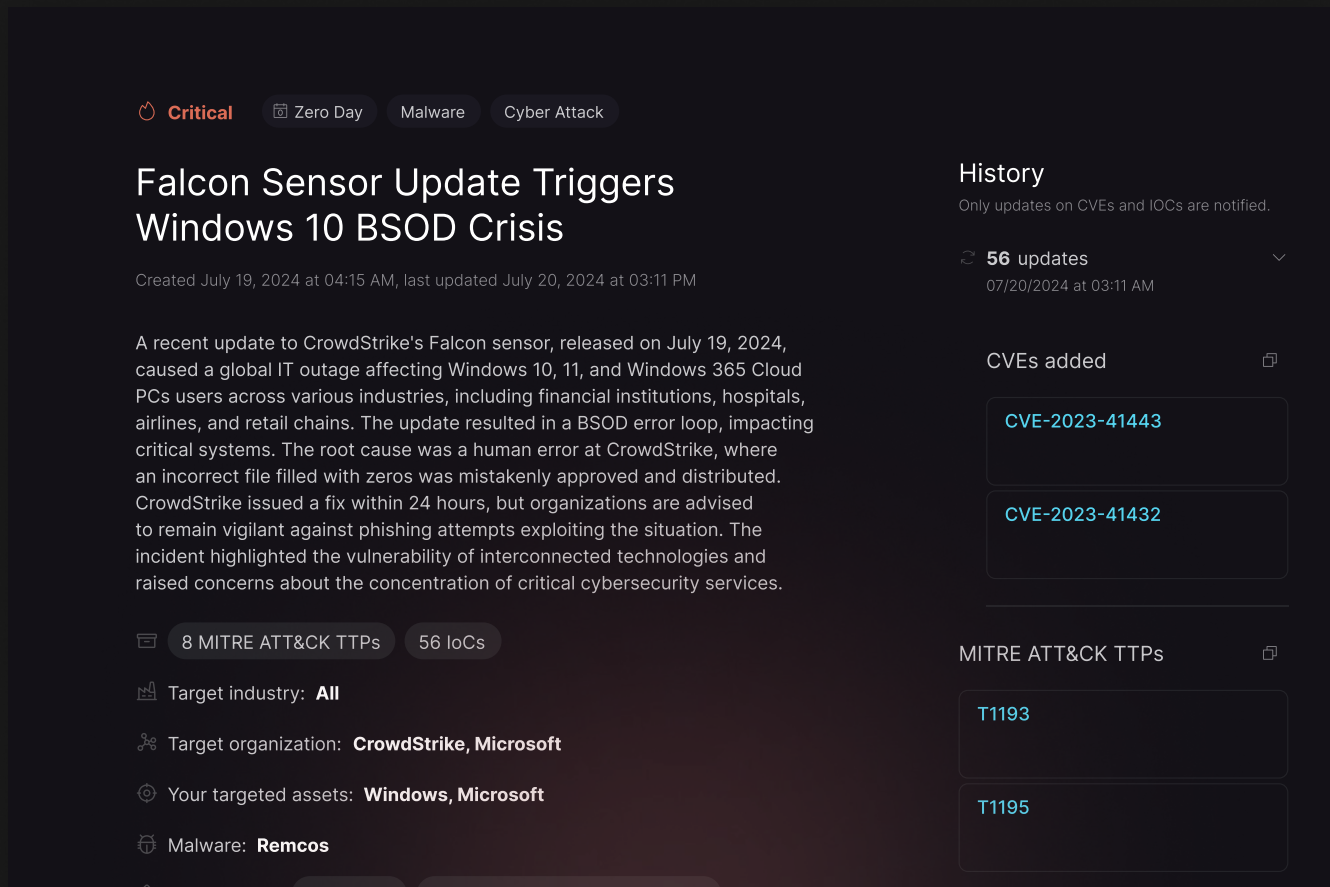


A powerful CTI team, inside your AI

Automate threat detection with the power of AI with embedded CTI



Critical Zero Day Malware Cyber Attack

Falcon Sensor Update Triggers Windows 10 BSOD Crisis

Created July 19, 2024 at 04:15 AM, last updated July 20, 2024 at 03:11 PM

A recent update to CrowdStrike's Falcon sensor, released on July 19, 2024, caused a global IT outage affecting Windows 10, 11, and Windows 365 Cloud PCs users across various industries, including financial institutions, hospitals, airlines, and retail chains. The update resulted in a BSOD error loop, impacting critical systems. The root cause was a human error at CrowdStrike, where an incorrect file filled with zeros was mistakenly approved and distributed. CrowdStrike issued a fix within 24 hours, but organizations are advised to remain vigilant against phishing attempts exploiting the situation. The incident highlighted the vulnerability of interconnected technologies and raised concerns about the concentration of critical cybersecurity services.

8 MITRE ATT&CK TTPs 56 IoCs

Target industry: **All**

Target organization: **CrowdStrike, Microsoft**

Your targeted assets: **Windows, Microsoft**

Malware: **Remcos**

History

Only updates on CVEs and IOCs are notified.

56 updates
07/20/2024 at 03:11 AM

CVEs added

- CVE-2023-41443
- CVE-2023-41432

MITRE ATT&CK TTPs

- T1193
- T1195

Fragmented data and constant alerts create blind spots for attacks. When key activities like vulnerability scanning, threat intelligence, and asset management are separated, you lose full visibility into your cyber risk. Axur's integrated Cyber Threat Intelligence (CTI) and External Attack Surface Management (EASM) close these gaps, providing full coverage, affordable intel, and maximum productivity. This unified approach helps you prioritize vulnerabilities, identify critical risks, and respond swiftly to threats.



Unified Threat Visibility



AI-Powered Efficiency



Real-time intelligence

Unleashing **Unmatched** Coverage, Speed, and Context

Cyberattacks

Identify and respond to attacks on your Attack Surface with actionable alerts to stay ahead of critical threats.

Proactive Threat Hunting

Conduct advanced searches to investigate risks related to credentials, domains, and emerging threats.

Vulnerabilities

Prioritize updates with alerts highlighting vulnerabilities, ensuring efficient application of critical patches.

Exposure Management (EASM)

Threat intel integrated with EASM for easy monitoring and response to emerging threats.

Let AI do the **hard work for you**, by searching, analyzing, and prioritizing relevant alerts

- Every day, Axur's CTI solution scans hundreds of sources, including news, groups, reports, and threat feeds.
- Its highly specialized LLM model sums up every relevant attack, threat, or vulnerability.
- It then filters everything relevant to your attack surface map and topics of interest.
- So it sends curated, actionable alerts with only what you really need to know, nothing else.



⊗ Before

11,000 alerts
faced by security teams daily

30 min
average time spent by an analyst in each alert

✓ With Axur

180x faster threat management by
correlating alerts to your Attack Surface

3x faster response freeing your
analysts to work strategically

Threat Landscape

[Generate summary ↗](#)

Trending in last 30 days related to my assets

Most impacted location

1st United States

2nd Canada

3rd Brazil

4th Russia

5th Ukraine

Assets

Identify your most vulnerable and frequently targeted assets, whether in your environment or globally, to prioritize protection.

Malware

Gain insights into malware families and related incidents, enabling faster responses to evolving threats.

Trending CVEs

Focus on critical vulnerabilities currently being exploited, with a prioritized view to target remediation.

Threat Actors

Access profiles of attackers, including their tactics and exploited vulnerabilities, to anticipate risks.

TTPs

Track trending adversary tactics and techniques to anticipate attack strategies and improve your defensive posture.

Industry Filter

Filter threats by industry to compare sector-specific risks and adapt your security strategy based on tailored insights.

Transform alerts into actionable insights

➔ Patch management made easy

Consolidate data to simplify patch prioritization, acting quickly on critical vulnerabilities.

➔ Strategic data for CISOs and security teams

Provide CISOs with actionable insights to prevent attacks and strengthen security posture.

➔ First-hand curated alerts

Stay ahead of emerging threats and promptly inform management for immediate action.

➔ No more endless tabs or contextless alerts

Eliminate the clutter of multiple tabs and receive only the most relevant, actionable alerts.

Revolutionize Your Cybersecurity with Unified EASM + CTI

Discover full visibility into your external digital footprint, helping you discover and secure all internet-facing assets. By integrating EASM with CTI, you gain an unmatched ability to manage vulnerabilities and respond to threats.

➔ Vulnerability Analysis

Compare assets against CVE databases to identify breaches, assess exploitability, provide CVSS scores, and verify digital certificates for authentication.

➔ Asset Discovery

Identify IPs, subdomains, and services for registered domains, enrich with Whois data, and detect open ports with running software and protocols.

The screenshot shows the Polaris interface, powered by AXUR. It displays a list of monitored assets. The interface includes a search bar, a table of assets, and a sidebar with navigation icons.

Asset	Type
one.ormus.com 14.123.412	Host
Safari	Technology
dev.ormus.com 123.123.321	Host
JQuery	Technology
nginx	Technology

The most powerful phishing detector

Boost your threat intelligence with Axur's Threat Hunting

➔ Proactive Investigations

Extensive data lake to hunt for threats
15 million signals analyzed daily

➔ AI-Assisted Searches

Simplify complex queries with AI-driven tools

➔ Comprehensive Coverage

Explore credentials, credit cards, domains and URLs

The screenshot shows the Threat Hunting interface. It features a table of credentials with columns for date, email, and password. The table is filtered by 'emailDomain=ormus.com,ormuspay.com'.

	emailDomain=ormus.com,ormuspay.com	Password
06/18/24 at 09:25	alice.williams@ormus.com	galaxyway2024
01/15/24 at 08:30	bob.smith@ormus.com	T9r\$zQ8#lU4w
02/22/24 at 03:45	carol.jones@ormuspay.com	Q1u\$M6z#X4cY
03/09/24 at 11:56	david.brown@ormus.com	thunderstorm007
04/17/24 at 06:15	emma.davis@ormuspay.com	Mountain@peak99
05/03/24 at 12:00	frank.miller@ormuspay.com	sandcastle456!
06/26/24 at 04:30	hank.moore@ormus.com	D6r#Y3w!T4lZ
07/14/24 at 08:00	mia.hall@ormuspay.com	L7m@Q1b&N8pX

Protect your assets and enhance your security posture now

START NOW WITH A DEMO

Discover all our solutions at axur.com



AXUR