



Endpoint agent

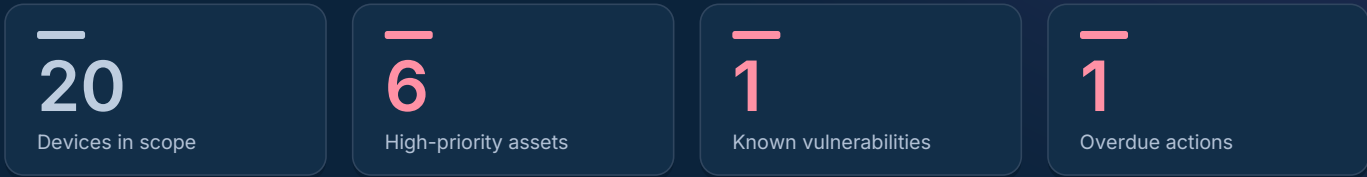
Device security, software updates and agent health

- 01 Overview
- 02 Assets
- 03 Intelligence
- 04 Actions

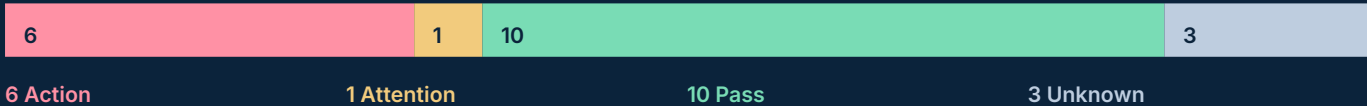
! Action required

Update Chrome on five devices and reconnect two agents.

Five browsers need an urgent security update. One device also lacks disk encryption.



ASSET STATUS



SECURITY CHECKS

Encryption		17/20 pass
Firewall		18/20 pass
Screen lock		17/20 pass
Protection		17/20 pass
Software		13/20 pass

Assessment coverage: 89 of 100 applicable checks returned a result. Grey indicates missing or outdated evidence.

TOP THREE PRIORITIES

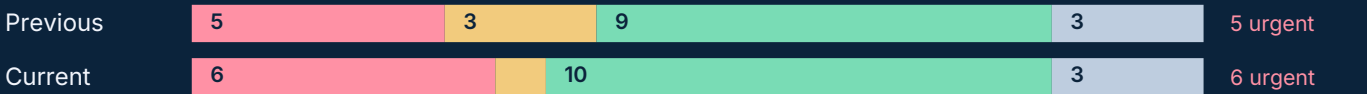
- 1 Update Google Chrome

Desktop support / 12 Sep
- 2 Enable disk encryption

Endpoint operations / 13 Sep
- 3 Apply the screen-lock policy

Desktop support / 16 Sep

CHANGE SINCE 06 SEPTEMBER



2 checks now pass; one new issue. Both assessments cover the same assets.

20 endpoints | 12 Windows + 8 macOS | Reports due every 24 hours in this example

Asset security overview

Security checks for each asset, ordered by priority.

01 Overview 02 Assets 03 Intelligence 04 Actions						
! Action ! Attention + Pass ? Unknown						
ASSET / PLATFORM	Encryption	Firewall	Screen lock	Protection	Software	
END-01 Windows	+ Pass	+ Pass	+ Pass	+ Pass	! Action	
END-02 Windows	+ Pass	+ Pass	+ Pass	+ Pass	! Action	
END-03 Windows	+ Pass	+ Pass	+ Pass	+ Pass	! Action	
END-04 Windows	+ Pass	+ Pass	+ Pass	+ Pass	! Action	
END-05 Windows	+ Pass	+ Pass	+ Pass	+ Pass	! Action	
END-06 Windows	! Action	+ Pass	+ Pass	+ Pass	+ Pass	
END-07 Windows	+ Pass	+ Pass	! Attention	+ Pass	+ Pass	
END-18 macOS	+ Pass	+ Pass	+ Pass	? Unknown	+ Pass	
END-19 macOS	? Unknown	? Unknown	? Unknown	? Unknown	? Unknown	
END-20 macOS	? Unknown	? Unknown	? Unknown	? Unknown	? Unknown	
END-08 Windows	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-09 Windows	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-10 Windows	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-11 Windows	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-12 Windows	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-13 macOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-14 macOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-15 macOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-16 macOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	
END-17 macOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass	

N/A checks are excluded from totals. Grey indicates missing or outdated evidence. Software checks do not cover every published vulnerability.

Next steps: address urgent findings first, then other outstanding issues. Repeat incomplete checks before confirming a pass.

Vulnerabilities and updates

Affected versions, exploitation status and recommended updates.

01 Overview

02 Assets

03 Intelligence

04 Actions

! Affected version confirmed

CVE-2023-4863

Google Chrome

A malicious WebP image may allow an attacker to run code through the browser.



CVSS 3.1



Known exploitation (KEV)



30-day likelihood



Affected devices

INSTALLED VERSION

116.0.5845.180

ORIGINAL FIX VERSION

116.0.5845.187

Affected versions: Chrome versions before 116.0.5845.187

Evidence: Device inventory identifies Google Chrome 116.0.5845.180.

RECOMMENDED UPDATE

Update Chrome to the latest supported release. Restart the browser and confirm that the updated version is running.

The original fix version is historical. Use the latest supported release.

Affected assets: END-01, END-02, END-03, END-04, END-05

Scope: 1 vulnerability across 5 assets. This report includes selected CVE examples.

Source dates: EPSS 2026-09-12; CISA KEV 2026-09-11; NVD updated 2026-06-17.

EPSS estimates the chance of this vulnerability being exploited in the next 30 days. It does not predict a breach of your organisation. EPSS percentile: 99.98%.

[NVD record](#) | [Google release advisory](#) | [EPSS explained](#) | [CISA KEV](#)

Remediation plan

Actions, responsible teams, deadlines and verification.

01 Overview	02 Assets	03 Intelligence	04 Actions
5 Open actions	1 Overdue	2 Checks now passing	
01 Update Google Chrome OVERDUE 12 Sep Install the supported update recommended on page 3 and confirm the version in use. END-F01 Desktop support 5 assets Open			
02 Enable disk encryption DUE 13 Sep Enable disk encryption and confirm that encryption has completed. END-F02 Endpoint operations 1 asset Open			
03 Apply the screen-lock policy DUE 16 Sep Apply the required screen-lock timeout and require a password when the device wakes. END-F03 Desktop support 1 asset Open			
04 Verify antivirus protection DUE 14 Sep Check that antivirus protection is active and restore its reporting to FIGQMS. END-F04 Agent support 1 asset Open			
05 Reconnect two endpoint agents DUE 14 Sep Reconnect both agents and collect a new full report from each device. END-F05 Agent support 2 assets Open			

Before closing an action: record the change and repeat the relevant check. Close the issue once the result confirms that the fix is effective.