BLACKSWAN CYBERSECURITY

THREAT ADVISORY
Google Chrome Zero-Day
(CVE-2026-85046)

September 4, 2026

Severity: Critical
CVSS: 8.8 (High)
CVE: CVE-2026-85046
Date Published: September 4, 2026
Status: Actively Exploited in the Wild
Affected Product: Google Chrome (Chromium-based browsers may also be affected pending vendor updates)

Executive Summary

Google released an emergency security update addressing **CVE-2026-85046**, a zero-day vulnerability in Chrome's V8 JavaScript and WebAssembly engine. Google confirmed that it has observed exploitation of this vulnerability in the wild. The flaw is a **Type Confusion** vulnerability that may allow a remote attacker to execute arbitrary code within Chrome's renderer sandbox by convincing a victim to visit a specially crafted webpage.

The vulnerability affects Chrome versions prior to:

- **Windows:** 152.0.7977.82 / 152.0.7977.83
- **macOS:** 152.0.7977.82 / 152.0.7977.83
- **Linux:** 152.0.7977.82

Organizations should prioritize patching all managed endpoints immediately and verify that Chromium-based browsers receive corresponding vendor updates.

Technical Summary

Vulnerability Details

CVE-2026-85046 is a Type Confusion vulnerability in the Chrome V8 JavaScript engine. Type confusion occurs when software incorrectly interprets one memory object as another type, creating opportunities for memory corruption and arbitrary code execution.

Researcher Salvatore Gulizia ("Serotav") identified the flaw and reported that compiler logic within Maglev and TurboFan optimization components could incorrectly map arrays using PACKED_ELEMENTS to PACKED_SMI_ELEMENTS, enabling arbitrary read/write operations within the JavaScript heap.

Potential Impact

Successful exploitation may allow an attacker to:

- Execute arbitrary code inside Chrome's renderer process.

- Read or manipulate memory contents.
- Bypass browser security controls.
- Deploy secondary malware payloads.
- Steal credentials and browser session tokens.
- Establish persistence through follow-on exploitation.

Attack Chain

Initial Access

Victim visits:

- Malicious website
- Compromised legitimate website
- Malvertising campaign
- Phishing lure containing malicious link

Exploitation

Specially crafted JavaScript triggers the V8 Type Confusion vulnerability.

Post-Exploitation

Potential attacker actions include:

- Browser memory access
- Credential theft
- Session hijacking
- Malware deployment
- Further privilege escalation via chained vulnerabilities

Google has not yet disclosed observed attack chains because exploitation activity is ongoing.

MITRE ATT&CK Mapping

ATT&CK Technique	Description
T1189	Drive-by Compromise
T1204.001	User Execution: Malicious Link
T1059.007	JavaScript Execution
T1068	Exploitation for Privilege Escalation
T1105	Ingress Tool Transfer
T1210	Exploitation of Remote Services
T1555	Credentials from Web Browsers

THREAT ADVISORY
Google Chrome Zero-Day
(CVE-2026-85046)

September 4, 2026

ATT&CK Technique	Description
T1539	Steal Web Session Cookie

Threat Hunting Guidance

High Priority Indicators

Investigate:

- Unexpected Chrome crashes.
- V8 renderer process crashes.
- Browser launches immediately followed by abnormal child processes.
- Downloads initiated from suspicious domains.
- Suspicious PowerShell or command shell activity spawned from browser-related processes.
- Browser-based exploitation followed by credential access attempts.

Process Monitoring

Look for:

```
chrome.exe
└── powershell.exe

chrome.exe
└── cmd.exe

chrome.exe
└── mshta.exe

chrome.exe
└── rundll32.exe

chrome.exe
└── wscript.exe
```

These behaviors are uncommon during normal browser activity.

Detection Opportunities

Microsoft Defender XDR

Chrome Spawning Suspicious Processes

```
DeviceProcessEvents
    | where InitiatingProcessFileName =~ "chrome.exe"
    | where FileName in~ (
```

```
"powershell.exe",
"cmd.exe",
"wscript.exe",
"cscript.exe",
"mshta.exe",
"rundll32.exe"
)
```

Suspicious Browser Downloads

```
DeviceFileEvents
    | where InitiatingProcessFileName =~ "chrome.exe"
    | where FileName matches regex @".*.(exe|dll|js|vbs|hta|ps1)$"
```

Browser-to-PowerShell Activity

```
DeviceProcessEvents
    | where InitiatingProcessFileName =~ "chrome.exe"
    | where FileName =~ "powershell.exe"
```

Sigma Rule

```
title: Chrome Suspicious Child Process
id: chrome-zeroday-child-process
status: experimental

    logsource:
    category: process_creation
    product: windows

    detection:
    selection:
    ParentImage|endswith:
    - '\chrome.exe'
    Image|endswith:
    - '\powershell.exe'
    - '\cmd.exe'
    - '\mshta.exe'
    - '\rundll32.exe'
    - '\wscript.exe'
```

- '\cscript.exe'

condition: selection

level: high

Indicators of Compromise (IOCs)

Currently Available

As of publication:

Known IOC Availability

- No public malicious domains released.
- No public exploit samples released.
- No public hashes released.
- No public infrastructure released.
- No public threat actor attribution released.

Google intentionally restricted technical details because exploitation is ongoing.

Affected Versions

Vulnerable

Versions prior to:
Windows:
152.0.7977.82 / .83

macOS:
152.0.7977.82 / .83

Linux:
152.0.7977.82

Remediation

Immediate Actions

Critical

1. Update Chrome immediately.
2. Force browser restart after update deployment.
3. Verify endpoint compliance.
4. Prioritize executive and privileged-user workstations.

5. Review EDR alerts for browser exploitation activity.

Enterprise Actions

- Deploy emergency patch via Intune, SCCM, GPO, or RMM platform.
- Verify browser version reporting organization-wide.
- Review web proxy logs for suspicious browsing activity.
- Increase monitoring for browser-launched child processes.

Version Verification

Chrome:

Settings
→ Help
→ About Google Chrome

Confirm version equals or exceeds:

152.0.7977.82

Blackswan Recommendation

Priority: P1 (Emergency Patching)

Recommended actions:

1. Validate Chrome version across all managed endpoints within 24 hours.
2. Force updates for all internet-facing and privileged-user systems.
3. Hunt for:
    - Browser-triggered PowerShell execution
    - Suspicious downloads
    - Browser crashes correlated with EDR alerts
4. Monitor Chromium-based alternative browsers (Edge, Brave, Opera, Vivaldi) for vendor-specific updates.
5. Issue an executive awareness bulletin advising employees to restart Chrome after updates are installed.