INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-20 06:54 UTC

CVE-2026-12348: Address bar spoofing in Arc Search for Android allows a remote attacker to display a trusted domain ...

CVE VULNERABILITY | HIGH | CVSS 7.4

SCC Item ID	SCC-CVE-2026-0341
Type	CVE Vulnerability
CVE ID	CVE-2026-12348
Severity	HIGH
CVSS Base Score	7.4
EPSS Score	0.0037 (29th percentile)
Affected Products	Arc Search for Android (specific version(s) not confirmed in available data)
Published	2026-06-17T10:14:49.290
Discovery Source	Nvd

Executive Summary

CVE-2026-12348 is a high-severity address bar spoofing vulnerability in Arc Search for Android that allows a remote attacker to display a legitimate-looking domain in the browser while serving attacker-controlled content. Organizations whose employees use Arc Search on Android-managed devices are exposed to targeted phishing attacks that bypass visual trust indicators users rely on. The business risk centers on credential theft and social engineering at scale, particularly against mobile device fleets without compensating controls.

Technical Analysis

CVE-2026-12348 affects Arc Search for Android and is classified under CWE-1021 (Improper Restriction of Rendered UI Layers or Frames), commonly known as UI redress. The vulnerability permits a remote attacker to manipulate the browser address bar display, presenting a trusted domain name while the rendered page content is fully attacker-controlled. CVSS base score is 7.4 (High); CVSS vector string is pending NVD publication. EPSS score is 0.00372 (28.8th percentile), indicating low current exploitation probability but meaningful phishing utility given the deception mechanism. MITRE ATT&CK techniques T1185 (Browser Session Hijacking) and T1566 (Phishing) are mapped to this vulnerability. No CISA KEV designation at time of publication. Specific affected version range and patch version were not confirmed in the available source data. Source NVD record:

https://nvd.nist.gov/vuln/detail/CVE-2026-12348 (T1, pipeline-verified).

Action Checklist

1. Step 1: Containment, Identify all managed Android devices in your MDM/EMM inventory running Arc Search. Restrict or block Arc Search usage on corporate-managed devices via MDM policy until a patched version is confirmed. Reference CIS 2.3: Address Unauthorized Software, treat unpatched Arc Search as unauthorized until remediated.
2. Step 2: Detection, Query MDM telemetry and mobile application management logs for Arc Search installation records across the Android device fleet. Review mobile proxy or Secure Web Gateway logs for anomalous browsing sessions originating from Arc Search on Android. There are no confirmed IOC signatures for this vulnerability in the available source data; detection relies on application inventory and session anomaly review. Reference NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Apply the vendor-issued patch for Arc Search on Android when The Browser Company publishes a remediated version. Version range and patch ID were not confirmed in available source data; monitor the official Arc release notes and NVD record (https://nvd.nist.gov/vuln/detail/CVE-2026-12348) for version confirmation. Until patched, enforce removal or disable via MDM per CIS 2.3.
4. Step 4: Recovery, After patch deployment, validate Arc Search version strings on all managed Android devices via MDM inventory. Confirm address bar behavior against a controlled test page to verify spoofing is no longer reproducible. Monitor Secure Web Gateway and mobile proxy logs for a minimum of 14 days post-remediation for anomalous session patterns. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident, Assess mobile application vetting processes: this vulnerability exposes a gap in pre-deployment security review of consumer browsers on corporate Android devices. Implement or strengthen mobile app allowlisting per CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.2 (Ensure Authorized Software is Currently Supported). Reinforce employee awareness training on address bar trust indicators, particularly the limits of visual domain verification on mobile browsers.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if Secure Web Gateway or mobile proxy log review identifies Arc Search sessions where users submitted credentials to domains that do not match the content server IP during the exposure window, as this indicates potential credential theft triggering breach notification obligations under applicable data protection regulations (e.g., GDPR, CCPA, HIPAA if PHI-adjacent systems were accessed).
Recovery Notes	After patch deployment, validate the patched Arc Search version string via MDM inventory on 100% of previously affected managed Android devices before restoring unrestricted browser access. Conduct a controlled address bar spoofing test using an analyst-controlled test page on a representative patched device to confirm CVE-2026-12348 is no longer reproducible. Maintain elevated Secure Web Gateway monitoring on Arc Search user-agent traffic for 14 days post-remediation, specifically watching for credential POST requests to anomalous or newly registered domains that would indicate an attacker continuing to exploit devices that did not receive the patch.

Forensic Artifacts	MDM application inventory export: Arc Search package name (com.thebrowser.browser) and versionName field across all enrolled Android devices — establishes exposure scope and confirms which devices ran the vulnerable version during the disclosure window. | Secure Web Gateway or mobile proxy session logs filtered on the Arc Search Android user-agent string: HTTP Host header, TLS SNI field, resolved destination IP, and HTTP POST events to login endpoints — the Host/SNI-to-IP mismatch is the network-observable signature of an active address bar spoofing session for CVE-2026-12348. | Android device browser cache and stored credential stores on devices where a spoofed session is suspected: Arc Search on Android stores browsing data under the app's data directory (/data/data/com.thebrowser.browser/), accessible via MDM remote collection or ADB backup on enrolled devices, to identify cached content from attacker-controlled origins. | Corporate identity provider (IdP) authentication logs: filter for successful logins originating from Android mobile user-agents during the exposure window, particularly from IP ranges inconsistent with the user's historical location — credential theft via a spoofed corporate login page would appear as a legitimate authentication event in the IdP. | DNS resolution logs from corporate DNS or mobile proxy for the exposure window: attacker-hosted spoofed pages for this type of address bar spoofing vulnerability typically use recently registered or lookalike domains as the actual content origin, which will appear in DNS logs even though the Arc Search address bar displayed the spoofed legitimate domain to the user.

Per-Action IR Details

Step 1: Containment — Identify all managed Android devices in your MDM/EMM inventory running Arc Search. Restrict or block Arc Search usage on corporate-managed devices via MDM policy until a patched version is confirmed. Reference CIS 2.3: Address Unauthorized Software — treat unpatched Arc Search as unauthorized until remediated.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, NIST AC-19 — Access Control For Mobile Devices

Compensating: If MDM policy enforcement is unavailable, use ADB in a device enrollment script to query installed packages: `adb shell pm list packages | grep -i arc` across enrolled devices. Maintain a manual spreadsheet of Arc Search installations flagged for removal, reviewed daily by one team member until MDM policy is enforced.

Evidence: Before restricting Arc Search via MDM policy, capture Arc Search's current version string from MDM inventory exports and any available mobile app usage logs from the Secure Web Gateway or mobile proxy to establish a baseline of devices that may have already encountered spoofed sessions. This is a client-side spoofing vulnerability — there is no server-side process to kill — so volatile state relevant to exploitation would be limited to active browser session data and any cached credentials stored by Arc Search on-device, which MDM remote wipe capability should address if compromise is confirmed.

Step 2: Detection — Query MDM telemetry and mobile application management logs for Arc Search installation records across the Android device fleet. Review mobile proxy or Secure Web Gateway logs for anomalous browsing sessions originating from Arc Search on Android. There are no confirmed IOC signatures for this vulnerability in the available source data; detection relies on application inventory and session anomaly review. Reference NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 — Event Logging, NIST AU-6 — Audit Record Review, Analysis, And Reporting, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Without a SIEM, export Secure Web Gateway or mobile proxy logs to CSV and use PowerShell or grep to identify Arc Search user-agent strings: `Select-String -Path proxy_logs.csv -Pattern 'Arc Search'`. Cross-reference resulting destination domains against known-legitimate corporate domains to identify sessions where the accessed IP or content did not match the displayed domain — the hallmark of this address bar spoofing mechanism. A two-person team can split the MDM inventory query from the proxy log review.

Evidence: Pull Secure Web Gateway or mobile proxy logs filtered on the Arc Search Android user-agent string, focusing on sessions where the HTTP Host header or TLS SNI field does not match the content server IP — this mismatch is the network-layer indicator of an active address bar spoofing session for CVE-2026-12348. Also capture MDM application inventory snapshots showing Arc Search version strings before any remediation action alters the device state.

Step 3: Eradication — Apply the vendor-issued patch for Arc Search on Android when The Browser Company publishes a remediated version. Version range and patch ID were not confirmed in available source data; monitor the official Arc release notes and NVD record (https://nvd.nist.gov/vuln/detail/CVE-2026-12348) for version confirmation. Until patched, enforce removal or disable via MDM per CIS 2.3.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 — Flaw Remediation, CIS 7.4 (IG1/IG2/IG3) — Perform Automated Application Patch Management, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software

Compensating: Without automated mobile patch management, establish a daily manual check of The Browser Company's official Arc release notes and the NVD record for CVE-2026-12348. When a patched version is confirmed, distribute the updated APK or trigger a managed Google Play update via MDM. Use ADB to verify the installed version post-update: `adb shell dumpsys package com.thebrowser.browser | grep versionName` and confirm it matches the vendor-confirmed patched release.

Evidence: Before pushing the patch or enforcing removal via MDM, capture a final MDM inventory export confirming Arc Search version strings on all affected devices — this documents the vulnerable state for post-incident records and any regulatory disclosure requirements. Because patch deployment alters application state on the device, this inventory snapshot is the last verifiable record of exposure scope prior to remediation.

Step 4: Recovery — After patch deployment, validate Arc Search version strings on all managed Android devices via MDM inventory. Confirm address bar behavior against a controlled test page to verify spoofing is no longer reproducible. Monitor Secure Web Gateway and mobile proxy logs for a minimum of 14 days post-remediation for anomalous session patterns. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 — Audit Record Review, Analysis, And Reporting, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process

Compensating: Without an enterprise proxy with automated alerting, configure a daily scheduled task or cron job to pull Secure Web Gateway logs and run a grep or PowerShell filter for Arc Search user-agent sessions where destination domains are newly registered or mismatched against corporate allow-lists — the pattern an attacker exploiting CVE-2026-12348 to harvest credentials post-patch-window would exhibit. For behavioral verification, use a controlled Android test device to navigate to an analyst-controlled spoofing test page and confirm the patched Arc Search version renders the correct domain without spoofing.

Evidence: During the 14-day monitoring window, retain Secure Web Gateway session logs filtered on the Arc Search Android user-agent, specifically capturing destination URL, HTTP Host header, TLS SNI, and resolved IP for each session. Any session where a corporate credential submission (HTTP POST to a login endpoint) occurred during the pre-patch window should be flagged for credential rotation, as this spoofing vulnerability's primary impact is credential theft through visually trusted but attacker-controlled pages.

Step 5: Post-Incident — Assess mobile application vetting processes: this vulnerability exposes a gap in pre-deployment security review of consumer browsers on corporate Android devices. Implement or strengthen mobile app allowlisting per CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.2 (Ensure Authorized Software is Currently Supported). Reinforce employee awareness training on address bar trust indicators, particularly the limits of visual domain verification on mobile browsers.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 2.1 (IG1/IG2/IG3) — Establish and Maintain a Software Inventory, CIS 2.2 (IG1/IG2/IG3) — Ensure Authorized Software is Currently Supported, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, NIST AC-19 — Access Control For Mobile Devices

Compensating: Without a formal mobile app vetting program, establish a documented manual review checklist for any consumer browser proposed for corporate Android use, covering: address bar integrity behavior, certificate validation handling, update cadence, and vendor security disclosure history. Distribute a one-page awareness brief to mobile device users specifically explaining that address bar spoofing vulnerabilities — as demonstrated by CVE-2026-12348 in Arc Search — mean that a correctly displayed domain is not sufficient proof of site authenticity on mobile browsers, and that corporate credential entry should be restricted to MDM-approved, allowlisted browsers.

Evidence: Produce a lessons-learned record documenting: the number of managed Android devices running Arc Search at detection, the duration of exposure window between vulnerability disclosure and MDM-enforced block, any Secure Web Gateway sessions flagged as potentially spoofed during the exposure period, and whether any credential submissions to login endpoints occurred via Arc Search during that window. This record supports both internal process improvement and any regulatory disclosure assessment if PII or corporate credentials were potentially exposed.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes, or URLs) are associated with active exploitation of CVE-2026-12348 in the available source data. Detection should focus on application inventory and behavioral signals. Query MDM/EMM platforms for Arc Search installations on Android devices and cross-reference against your authorized software inventory (CIS 2.1). In Secure Web Gateway or mobile proxy logs, look for sessions from Arc Search user-agent strings navigating to high-value targets (corporate SSO portals, financial services, SaaS login pages) that subsequently present anomalous redirect chains. SIEM rule suggestion: alert on Arc Search user-agent strings combined with HTTP 200 responses from domains not matching the requested host header, if your proxy captures that telemetry. NIST AU-2 and AU-6 apply for log collection and review cadence. No specific event IDs or log query syntax can be provided without confirmed vendor logging documentation.

Framework Mappings

MITRE-ATTACK

- **T1185** — Browser Session Hijacking
- **T1566** — Phishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1185	Browser Session Hijacking	Collection
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-12348	T1
CVE-2026-12348 - Vulnerability Details - OpenCVE	https://app.opencve.io/cve/CVE-2026-12348	T3
CVE-2026-12348 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-12348	T3
CVE-2026-12348 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
CVE-2026-34448 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-34448	T1

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-20 06:54 UTC by TJS Security Command Center