Security Bulletin

Our latest updates on Security

Welcome to our Arc Security Bulletin. Here you'll find the most up to date information on recent security fixes. We get into the weeds a little here, if you have any questions you can always find us on security@thebrowser.company.

Follow on Twitter

Report a Vulnerability

June 16, 2026

CVE-2026-12348: Address Bar Spoofing in Arc Search for Android (window.open race condition)

- **Summary:** Address Spoofing risk in ArcSearch on Android
- **CVE ID:** CVE-2026-12348
- **Advisory Release Date:** 2026/06/16
- **Affected Version:** ArcSearch on Android version <1.12.9

- **Severity:** High

Details

If you're using ArcSearch for Android versions prior to 1.12.9, it could display a different domain in the address bar than the content being shown. This could increase spoofing risk after a user interaction.

Severity

The Browser Company rates this issue High with a CVSS v3.1 base score of 7.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). This reflects our internal assessment—please evaluate applicability within your environment.

Affected Versions

ArcSearch on Android versions < 1.12.9

What do I need to do?

Update ArcSearch on Android to the latest available version. Any version 1.12.9 or newer contains the fix.

Credit

The Browser Company thanks alfazhossain for reporting this issue through our vulnerability rewards program.

March 20, 2026

CVE-2026-2378: ArcSearch Android Omnibar Spoof

- **Summary:** Address Spoofing risk in ArcSearch on Android
- **CVE ID:** CVE-2026-2378
- **Advisory Release Date:** 2026/03/20
- **Affected Version:** ArcSearch on Android version <1.12.7
- **Severity:** High

Details

If you're using ArcSearch for Android versions prior to 1.12.7, it could display a different domain in the address bar than the content being shown. This could increase spoofing risk after a user interaction.

Severity

The Browser Company rates this issue High with a CVSS v3.1 base score of 7.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). This reflects our internal assessment—please evaluate applicability within your environment.

Affected Versions

ArcSearch on Android versions < 1.12.7

What do I need to do?

Update ArcSearch on Android to the latest available version. Any version 1.12.7 or newer contains the fix.

Credit

The Browser Company thanks moch_azril for reporting this issue through our vulnerability rewards program.

December 19, 2025

CVE-2025-14809: Address bar spoofing risk; navigation trigger URI confusion on ArcSearch (Android)

- **Summary:** Address Spoofing risk in ArcSearch on Android
- **CVE ID:** CVE-2025-14809
- **Advisory Release Date:** 2025/12/19
- **Affected Version:** ArcSearch on Android version <1.12.6
- **Severity:** High

Details

If you're using ArcSearch for Android versions prior to 1.12.6, it could display a different domain in the address bar than the content being shown. This could increase spoofing risk after a user interaction.

Severity

The Browser Company rates this issue High with a CVSS v3.1 base score of 7.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). This reflects our internal assessment—please evaluate applicability within your environment.

Affected Versions

ArcSearch on Android versions < 1.12.6

What do I need to do?

Update ArcSearch on Android to the latest available version. Any version 1.12.6 or newer contains the fix.

Credit

The Browser Company thanks moch_azril for reporting this issue through our vulnerability rewards program.

December 19, 2025

CVE-2025-14812: Address bar spoofing risk; iframe-triggered URI navigation on Arc Search (iOS)

- **Summary:** Address Spoofing risk in ArcSearch on iOS
- **CVE ID:** CVE-2025-14812
- **Advisory Release Date:** 2025/12/19
- **Affected Version:** ArcSearch on iOS versions prior to 1.45.2
- **Severity:** High

Details

If you're using ArcSearch for iOS versions prior to 1.45.2, it could display a different domain in the address bar than the content being shown after an iframe-triggered URI-scheme navigation. This could increase spoofing risk.

Severity

The Browser Company rates this issue High with a CVSS v3.1 base score of 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). This reflects our internal assessment—please evaluate applicability within your environment.

Affected Versions

ArcSearch on iOS versions < 1.45.2

What do I need to do?

Update ArcSearch on iOS to the latest available version. Any version 1.45.2 or newer contains the fix.

Credit

The Browser Company thanks syarif07 for reporting this issue through our vulnerability rewards program.

December 3, 2024

Expanding our security program with HackerOne

Hi there, Cory here! I'm a Security Engineer at The Browser Company. Today, I'm excited to share some significant updates about our security program and our continued commitment to protecting Arc and our members.

Two months ago, we launched a bug bounty program as part of our ongoing investment in security. The response has been incredible, and we want to thank everyone who contributed to help make Arc even more secure. Building on this momentum, I'm thrilled to announce that we're taking the bug bounty program to the next level by partnering with HackerOne.

Why HackerOne?

HackerOne is the world's largest community of trusted ethical hackers. Partnering with them was a natural next step in our commitment to making Arc as secure as possible. This partnership will provide researchers with a streamlined platform for submitting vulnerabilities, ensuring faster response times, while offering a more structured reward system.

The migration to HackerOne will help us:

- Provide a better experience for security researchers
- Streamline our vulnerability reporting and triage process
- Ensure consistent and timely communications with researchers
- Scale our bug bounty program more effectively

Growing our Security Team

As The Browser Company continues to evolve, so does our investment in security. In fact, we're looking to double our security team. If you're passionate about browser security, love solving complex problems, and want to develop the foundation of security for our next generation AI-assistant, we'd love to hear from you. Check out our open positions on our career page.

Looking Forward

The first two months of the bug bounty program have inspired us to do more work with the broader security community. Moving to HackerOne is just one of many steps we're taking to strengthen our security posture. We're committed to our practice of transparent communication about security issues and ultimately maintaining the trust our members place in us.

For security researchers interested in participating in our program, you can now report issues directly through The Browser Company's (BCNY) HackerOne page. Our bug-bounty@thebrowser.company reporting method will now route you through HackerOne.

Again, we want to thank everyone who has contributed to our security program so far. Your work helps make Arc better and more secure for everyone.

Questions?

If you have any questions about this transition or our security program in general, please reach out to us at security@thebrowser.company.

November 12, 2024

Windows Site Settings Bypass - CVE-2024-52928

On Nov 4, 2024, we became aware of a vulnerability in how Windows handled site settings, allowing a site that had previously been granted permissions the ability to request new permissions and have them be automatically granted. We resolved this issue on Nov. 4 2024.

What happened?

Arc on Windows was not properly handling follow up permissions requests for websites that had previously requested permissions. This was due to a bug in how Arc

on Windows handled the site settings state for websites. This bug allowed a site to request additional permissions which were granted when the user clicked anywhere on the page, bypassing the explicit permission grant that the user should give. Permission denies were still respected and we would properly display the permissions popup for all websites.

Who was affected?

Arc on Windows versions ≤ 1.26.0 are vulnerable and need to update. No macOS versions were affected by this issue.

What mitigations have we put into place?

On disclosure, we immediately patched the issue with how Windows handles additional permissions requests for sites that previously had permissions granted by the user. This fix went out in hotfix 1.26.1 on Arc for Windows.

What do I need to do?

Please update to a version >= 1.26.1 on Windows

Credit

Thank you to Bharat(mrnoob) for reporting this finding.

November 05, 2024

Javascript Boost Full Disk Access

On October 7, 2024, we were alerted to a vulnerability in legacy Boosts. We resolved this issue on Oct. 8 2024, and after a thorough review, the team confirmed that no members were affected.

What happened?

A researcher informed us of a potential vulnerability involving legacy boosts where someone could create a specific link within an Easel that, if clicked twice: once in the attacker controlled Easel and a second time in the an Arc controlled confirmation, could install a legacy boost that had write access to a user's local disk.

Only Arc on Mac had support for legacy boosts as it was never implemented on Arc on Windows.

Who was affected?

Based on our investigation, no members have been affected. An analysis of all Easel data confirmed no Easels contained an embedded legacy boost, outside of the Easels created for testing this bypass.

What mitigations have we put into place?

On disclosure, we immediately patched the existing backend sanitization regular expressions used for embedding URLs in Easels. We also added further backend rules to enforce specific URL schemas for embeddings and to ensure all Easels are properly sanitized.

Additionally, as of MacOS Arc 1.66.0, the legacy boost feature has been completely removed. Although this removal wasn't necessary to prevent the disclosed vulnerabilities, we deemed it a prudent security measure given the feature's low usage and potential risks.

What do I need to do?

No action is necessary for members to be protected. All updates were applied to our backend infrastructure, and all backend system patches are automatically and immediately applied to all members. While all members are already protected, we always recommend keeping your Arc up to date.

Credit

Thank you to RenwaX23 for reporting this finding.

September 27, 2024

Easel URL Embed Issue - CVE Pending

On Sept. 23 2024 we were alerted to a URL embed issue with Easels. This was resolved on Sept. 24 2024.

What happened?

Arc has a feature called Easels that allow you to create a page that has custom text, pictures, and embed URLs from your favorite sites. A vulnerability in Easels could allow a shared Easel to masquerade as another site when loaded in other browsers. Easels loaded in other browsers rely on fallback HTML rendering via arc.net that uses

regular expressions to whitelist specific video providers which allowed for arbitrary content to be displayed on URLs starting with arc.net/e/.

Easels are created in Arc, which properly validates submitted URLs. However, a malicious actor could potentially modify their own Easels and bypass the client validation by making an API request directly to the backend.

Who was affected?

Based on our investigation, no users have been impacted by this issue. An analysis of all Easel data confirmed no Easels with a video embed used as an iframe, outside of the Easel created by the security researcher. All embedded video URLs passed the regex we use to whitelist video providers.

What mitigations have we put into place?

On disclosure, we patched the existing backend sanitization regexes that are used for embedding URLs in Easels. We also added further backend rules to enforce specific URL schemas for video embeddings and to ensure all Easels had a standard ID format, preventing a convincing URL like arc.net/e/download from existing.

What do I need to do?

No action is necessary for members to be protected. All updates were applied to our backend infrastructure, and all backend system patches are automatically and immediately applied to all users. While all members are already protected, we always recommend keeping your Arc up to date.

Credit

Thank you to Eva who reported this issue.

September 27, 2024

How we're investing in security at The Browser Company

Hi there, Josh here, CEO of The Browser Company — welcome to our new Arc Security Bulletin, the home for our most up-to-date security advisories and incident reports for Arc.

I wanted to start by sharing a one week update on the Incident Report my cofounder Hursh wrote last week about a significant security vulnerability in Arc. Although no users were affected by the vulnerability, we've taken this moment to level up our security and incident response practices across the company.

In that post, we shared nine changes that we were making to our security practices. Our team has since been working around the clock to do those things and more. As I've shared, talk is cheap in these moments and action is all that matters. Therefore I'd like to share the concrete changes we've made and will be continuing to make at The Browser Company.

Transparent and proactive communication

We've always strived to communicate transparently, thoughtfully, and clearly with our membership as we build Arc — and security is no different. Today, we're releasing a new Security Bulletin (what you're reading now), which will serve as the source of truth for all security incident reports. That includes technical write-ups, CVE numbers, mitigations, and impact assessments.

Furthermore, we have started and will continue to include all security-focused fixes in our release notes, which can always be found in the Arc Resource Center for Mac, Windows, and Mobile.

Bug Bounty Program

Secondly, we are launching the Arc Bug Bounty Program. Just as we've built Arc with our members, we recognize the invaluable role that the security research community plays in fortifying products and platforms like ours. You'll find details for the Arc Bug Bounty Program here, including the rewards and submission guidelines. We've strived to make it the best it can be and know it will evolve — we'd always love to hear from you.

Alongside our new program, we have also taken the opportunity to increase the payment to the researcher for last week's issue, aligning it with our new guidelines and our appreciation as a team.

Further mitigations for CVE-2024-45489

The root issue behind CVE-2024-45489 was patched on August 26, 2024, with no members affected. Over the past week, our team has continued to ship additional

remediations and precautions specifically related to this incident, specifically:

- We've disabled Boosts with Javascript from being automatically enabled across synced devices — released in Arc 1.61.2.
- We've enabled a new global toggle to disable all Boost-related features in Advanced Settings — released in Arc 1.61.2.
- We've engaged an external audit firm to perform a comprehensive audit of our backend systems — starting with the area of access-control list (ACLs) and including all code changes in features related to recent vulnerabilities.
- We are in the process of enabling MDM configuration to disable Boosts for entire organizations, which the team will be releasing in the coming weeks.

Internal process improvements

Inside the team, we're implementing new practices to help identify potential vulnerabilities earlier, and evolving our engineering posture to further enhance security while developing new features.

- **New development guidelines.** Our development team is instituting new guidelines including additional code reviews, defense-in-depth coding practices, and secure-by-design principles.
- **Increasing security-specific code audits.** In addition to our existing code reviews, we will implement additional security audits. These audits will be conducted by our Security team and outside auditing firms.
- **Improving our approach to external audits.** We are reconfiguring the way we partner with external security audit firms. They will be involved earlier in the release process to help with secure design feedback, and will undertake full code reviews of new features once they are completed. We will also increase the priority of potential issues that are surfaced, and create a new escalation path.
- **Growing our internal security engineering team.** We are welcoming a new hire to our Security team this coming Monday, with another role in the pipeline. If you're interested in Security or SRE roles at The Browser Company we'd love to hear from you.
- **Overhauling our incident response process.** We are revamping our internal incident response processes to enable faster response times and improved communication. We're strengthening the tracking and ownership

of issues, revisiting our hotfix processes, and looping in our communications team as early as possible. We want to share information about security fixes with members as soon as possible, and for security researchers to have as strong of an experience as possible when working with our team to fix vulnerabilities.

- **Committing to reducing technical debt.** Building Arc has been a journey, and browsers are a complex piece of technology. As we continue on this journey, we want to be mindful that complexity can lead to security issues. We'll be carefully reviewing our code base to find areas where we can reduce attack surface and improve overall code health. We've always been an experimental organization at The Browser Company, this change is important if we want to keep nimble with product development.

Showing up with heartfelt intensity

As a founder, it's deeply personal to face up to an incident like this. This was our first major discovered vulnerability but—and I wince when I say it—it won't be the last. All mature products unfortunately deal with these. How you handle and communicate them, and especially how you learn and grow from them, is what makes the difference in trusting a company and a product over the long term. Thanks for bearing with us on this particular bump in the road of Arc's journey.

September 20, 2024

CVE-2024-45489 Incident Report

Hursh here, CTO and Cofounder of The Browser Company. We want to let all Arc users know that a security vulnerability existed in Arc prior to 8/25/24. We were made aware of a vulnerability on 8/25, it was fixed on 8/26. This issue allowed the possibility of remote code execution on users' computers. We've patched the vulnerability immediately, already rolled out the fix, and verified that no one outside of the security researcher who discovered the bug has exploited it. **This means no members were affected by this vulnerability, and you do not need to take any action to be protected.**

Despite the low impact, this is the first serious security incident in Arc's lifetime. We're taking this moment to upgrade everything from our internal security reviews, to our bug bounty program, to our communications with Arc members on such incidents.

Thanks to xyz3va for their private report and subsequent public writeup. Internal investigations are ongoing, but in the meantime want to share the technical details of the vulnerability.

What happened?

Arc has a feature called Boosts that allows you to customize any website with custom CSS and Javascript. Since running arbitrary Javascript on websites has potential security concerns, we opted not to make Boosts with custom Javascript shareable across members, but we still synced them to our server so that your own Boosts are available across devices.

We use Firebase as the backend for certain Arc features (more on this below), and use it to persist Boosts for both sharing and syncing across devices. Unfortunately our Firebase ACLs (Access Control Lists, the way Firebase secures endpoints) were misconfigured, which allowed users Firebase requests to change the creatorID of a Boost after it had been created. This allowed any Boost to be assigned to any user (provided you had their userID), and thus activate it for them, leading to custom CSS or JS running on the website the boost was active on.

Who was affected?

No Arc members were affected by this vulnerability. We did an analysis of our Firebase access logs and confirmed that no creatorIDs had been changed outside those changed by the security researcher.

Mitigation

xyz3va's writeup goes into more detail about the steps to mitigate this vulnerability. On disclosure, we worked with them to patch our ACLs to fix this vulnerability, and confirmed the fix with them the following day. Considering the scale of the vulnerability, we also submitted for a CVE and, while we haven't yet set up a formal bug bounty program, we worked to award a bounty for the issue.

Next steps

This was the first vulnerability of this scale that we've seen in Arc, and we really want to use this as an opportunity to improve how we respond to and disclose security vulnerabilities.

In terms of this specific issue, we are making a number of changes to avoid this moving forward and to improve our communication around security vulnerabilities:

- We've fixed the issues with leaking your current website on navigation while you had the Boost editor open. We don't log these requests anywhere, and if you didn't have the Boosts editor open these requests were not made. Regardless this is against our privacy policy and should have never been in the product to begin with.
- We're disabling Javascript on synced Boosts by default. Any Boost with custom Javascript that was created on another device will need to be explicitly enabled moving forward.
- We're adding MDM configuration to disable Boosts for your entire organization.
- We're moving off Firebase for new features and products, mitigating future issues with ACLs.
- We're doing an emergency and more in-depth external audit of our existing Firebase ACLs to ensure there are no other vulnerabilities, in addition to our external security audits every six months. We are still planning to move off Firebase for all future features.
- We're establishing a security bulletin with clear comms around vulnerabilities, mitigations, and who was affected. We've been really inspired by Tailscale's excellent security reporting, and we want to hold ourselves to the same standard.
- We're establishing clearer guidelines for bounties, specifying which severity levels warrant particular reward amounts.
- We're adding security mitigations to our release notes. Since this was a server-side fix, it didn't occur to us to include it in our client release notes, but since that's the major venue where members get information about updates in Arc, they should be included there.
- We're also bolstering our security team, and have hired a new senior security engineer.

If you have any questions please reach out to us at security@thebrowser.company. As a team we will be using this moment to grow as a company and as engineers. We will integrate all of your questions, thoughts, and feedback into our larger discussions and full retrospective.

If you have any questions or suggestions, give us a shout at help@arc.net →