Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

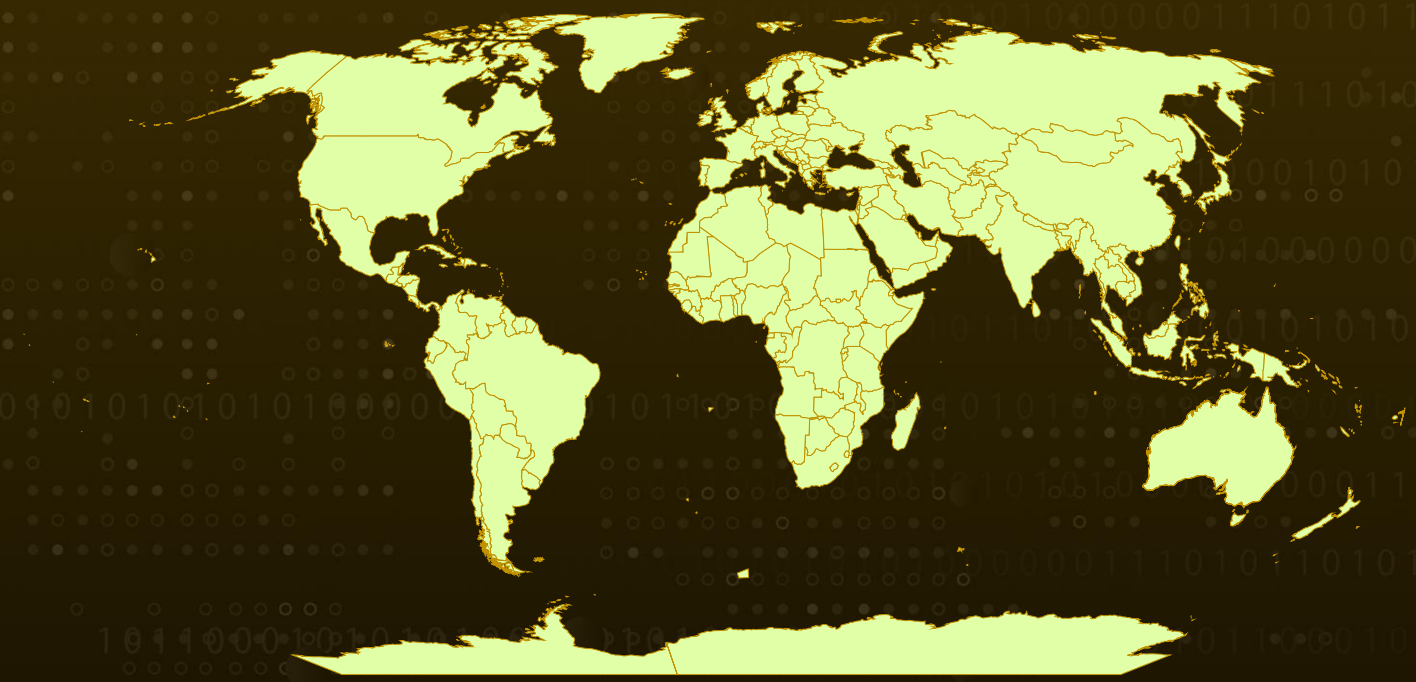
18 Years of Unresolved Threat: 0.0.0.0 Day Vulnerability in Major Browsers

Date of Publication	Admiralty Code	TA Number
August 9, 2024	A1	TA2024305

Summary

First Observed: 2006
Affected Browsers: Chromium, Firefox, Safari
Affected OS: Linux and macOS
Targeted Region: Worldwide
Attack: The "0.0.0.0 Day" vulnerability is a critical security flaw that affects major web browsers like Chromium, Firefox, and Safari, allowing malicious websites to exploit localhost APIs through the 0.0.0.0 IP. This vulnerability, which has been exploited since 2006, bypasses traditional browser security mechanisms, enabling attackers to gain unauthorized access to internal applications on macOS and Linux.

Attack Regions



Attack Details

#1 The "0.0.0.0 Day" vulnerability is a critical security flaw that permits malicious websites to exploit localhost APIs directly from within a browser. Since 2006, various attack campaigns have exploited this vulnerability by leveraging the fact that browsers prioritize responses over requests, leaving them susceptible to malicious JavaScript embedded in attacker-controlled websites.

#2 Despite the passage of eighteen years, the bug remains unresolved, having been repeatedly closed, reopened, and reprioritized as "severe" or "critical," with documented cases of exploitation in the wild. The impact of the 0.0.0.0 Day vulnerability is compounded by its wide reach, affecting all major web browsers, including Chromium, Firefox, and Safari, and enabling external websites to communicate with software running locally on macOS and Linux.

#3 Notably, it does not impact Windows devices, as Microsoft blocks the IP address at the operating system level. This vulnerability is particularly alarming because it bypasses conventional browser security mechanisms designed to shield users from remote threats. Attackers can exploit this by directing a browser to interact with services running on localhost, thereby gaining unauthorized access to internal applications that are typically inaccessible from the outside.

#4 Exploitation typically involves crafting a malicious website that triggers the browser to make requests to 0.0.0.0. Once these requests are initiated, the attacker can interact with localhost services as if they were part of the local network. This can lead to serious consequences, particularly in environments where critical applications or services are running on localhost.

#5 Attackers can carry out various malicious activities, such as accessing sensitive information, altering configurations, or even executing remote code, depending on the services running on the target's local machine. Recently, there has been a significant increase in the number of public websites communicating with 0.0.0.0, with the number now reaching approximately 100,000.

#6 The 0.0.0.0 Day vulnerability is actively exploited in the wild, with notable cases including the ShadowRay campaign, documented in March 2024, which targets AI workloads running locally on developers' machines. Another recent example is a campaign targeting Selenium Grid, discovered last month. Additionally, the "ShellTorch" vulnerability reported in October 2023 involved the TorchServe web panel being bound to the 0.0.0.0 IP address by default instead of localhost, exposing it to malicious requests.

Recommendations

Verify HOST Headers: Validate HOST headers in incoming requests to protect against DNS rebinding attacks that could potentially target localhost.

Be Aware of Browser Routing: Recognize that browsers can route HTTP requests to internal IP addresses, including localhost. Until browser vendors fully implement fixes, remain vigilant about this potential vulnerability in your app development.

Implement CSRF Tokens: Use Cross-Site Request Forgery (CSRF) tokens in your applications, including Intranet Applications, to prevent unauthorized actions performed on behalf of users.

Prepare for Browser-Specific Solutions: Google Chrome is continuing its gradual rollout to block access to 0.0.0.0, with full implementation anticipated by version 133. Mozilla Firefox is focusing on implementing PNA (Private Network Access) headers to address risks related to 0.0.0.0, while applying temporary fixes until PNA is fully in place. Meanwhile, Apple Safari will introduce additional IP checks to block access to 0.0.0.0 in version 18, set to be released with macOS Sequoia.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0007** Discovery
TA0010 Exfiltration	**TA0040** Impact	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter
T1046 Network Service Discovery	**T1567** Exfiltration Over Web Service	**T1505** Server Software Component	**T1565** Data Manipulation
T1005 Data from Local System			

References

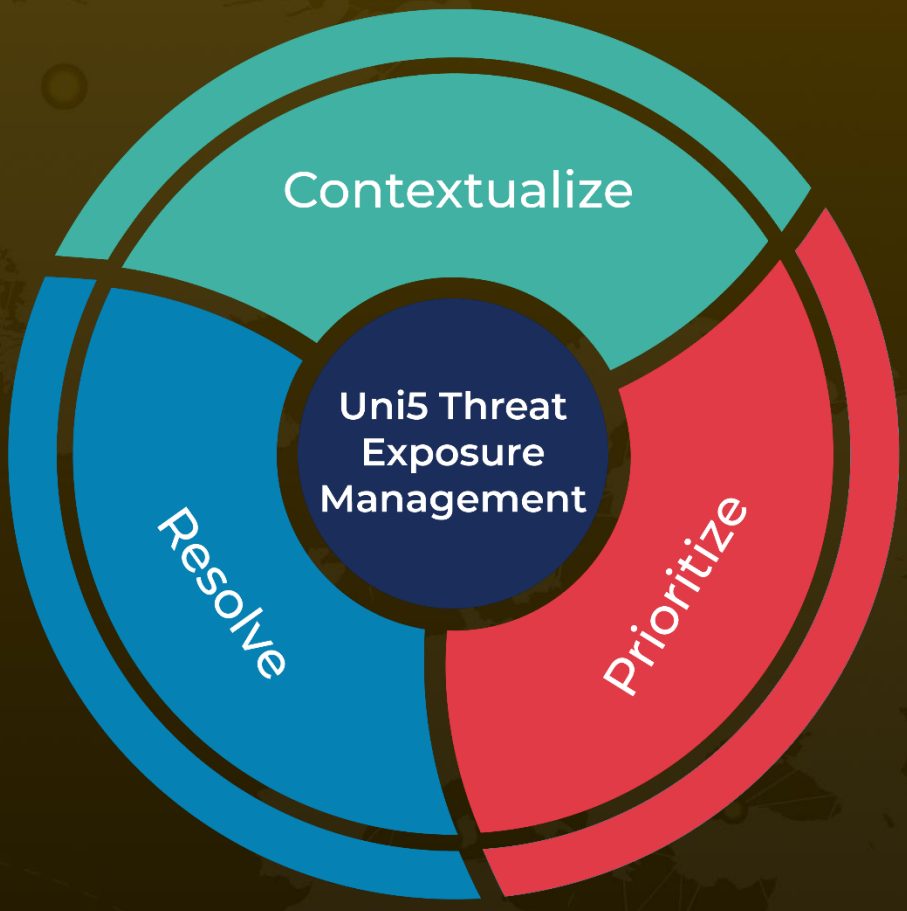
https://www.oligo.security/blog/0-0-0-0-day-exploiting-localhost-apis-from-the-browser

https://hivepro.com/threat-advisory/cracking-shelltorch-vulnerabilities-exposing-torchserve-to-rce/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 9, 2024 • 6:00 AM

More at www.hivepro.com