Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Critical Vulnerability in Openfire Admin Console Actively Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
August 25, 2023	A1	TA2023346

Summary

First Seen: May 2023
Affected Platforms: Ignite Realtime Openfire
Impact: The vulnerability (CVE-2023-32315) in Ignite Realtime Openfire, enabling unauthorized access to privileged pages. Attackers exploit this by bypassing authentication, prompting immediate updates for affected servers.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Ignite Realtime Openfire	✗	✓	✓

Vulnerability Details

#1 CVE-2023-32315 is a path traversal vulnerability affecting the Openfire admin console, a web-based application. This vulnerability allows an unauthenticated attacker to access restricted pages in the Openfire Admin Console, including the ability to create an administrative user and upload a plugin.

#2 The vulnerability can be exploited by sending a specially crafted request to the Openfire admin console. The vulnerability has been exploited in the wild, and there are a number of public exploits available for this vulnerability.

#3 Some public exploits involve creating an admin user to gain access, but a more stealthy approach extracts session and CSRF tokens, allowing the attacker to upload a plugin without creating an admin account. This method avoids security audit logs, leaving minimal evidence.

#4

This vulnerability affects all versions of Openfire that have been released since April 2015, starting with version 3.10.0. Around 50% of accessible Openfire servers are running affected versions. Users are advised to update to the latest versions promptly to mitigate potential threats. The flaw's impact underscores the need for improved network-based detection and security measures against path traversal vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-32315	Openfire versions: 3.10.0, 3.10.1, 3.10.2, 3.10.3, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.3.0, 4.3.1, 4.3.2, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, 4.6.0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Patch your server to the latest version: Ignite Realtime has released patched versions of Openfire that address this vulnerability. You can download the latest version from the Openfire website.

Disable the admin console: If you do not need to use the admin console, you can disable it to prevent attackers from exploiting this vulnerability. To do this, edit the openfire.xml file and set the enableAdminConsole property to false.

Bind Admin Console to Loopback Interface: Configure the admin console webserver to bind exclusively to the loopback interface (e.g., 127.0.0.1). This way, it's accessible only from the server itself, reducing the attack surface. Note that this could impact certain plugin functionalities relying on the admin console.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0009 Collection	TA0002 Execution	TA0040 Impact	T1556 Modify Authentication Process
T1068 Exploitation for Privilege Escalation	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1098 Account Manipulation
T1136 Create Account	T1505.003 Web Shell	T1505 Server Software Component	T1070.004 File Deletion
T1070 Indicator Removal	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits

Patch Details

Upgrade Openfire versions to 4.6.8, 4.7.5, 4.8.0 or newer versions

Link:
https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm

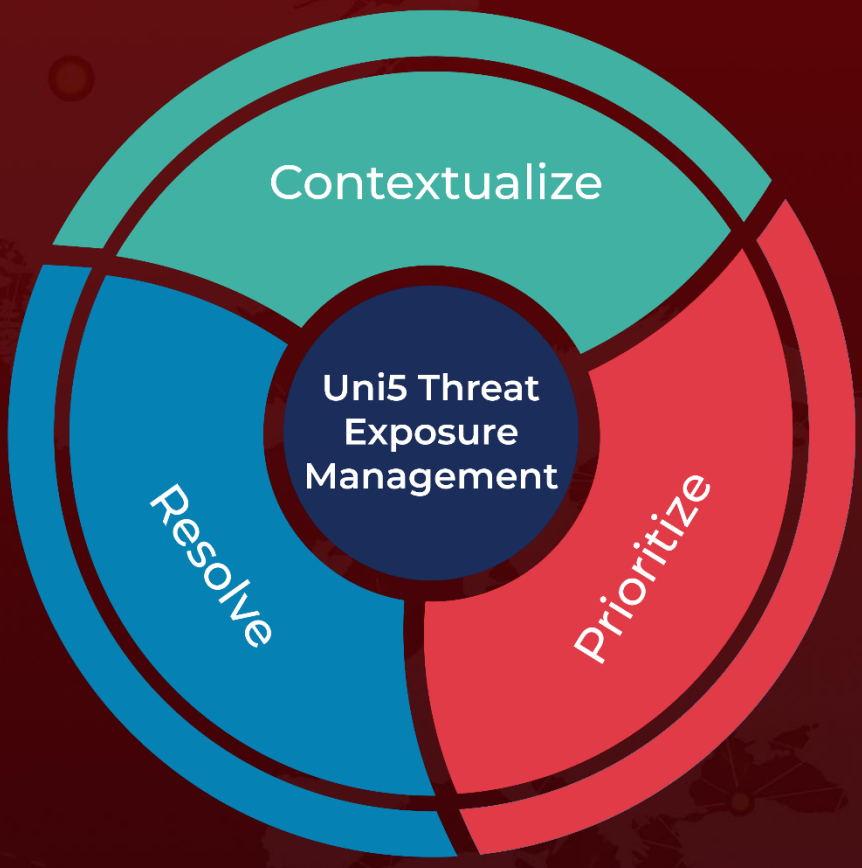
References

https://vulncheck.com/blog/openfire-cve-2023-32315

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 25, 2023 • 6:45 AM

More at www.hivepro.com