Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Fortinet FortiWLM Vulnerability Exposes Admin Controls to Attackers

Date of Publication	Admiralty Code	TA Number
December 20, 2024	A1	TA2024469

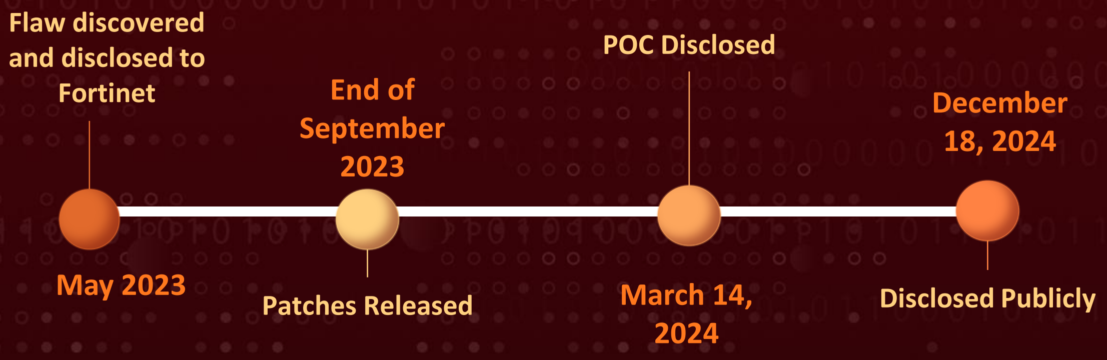
Summary

First Seen: May 2023
Affected Products: Fortinet FortiWLM
Impact: Fortinet has recently revealed a critical vulnerability in its Fortinet Wireless Manager (FortiWLM) that could allow remote attackers to fully compromise devices. This flaw, identified as CVE-2023-34990, stems from a relative path traversal vulnerability, enabling attackers to execute unauthorized code or commands through specially crafted web requests. Discovered in May 2023, the issue was patched by the end of September 2023 but was publicly disclosed in December 2024.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-34990	Fortinet FortiWLM Relative Path Traversal Vulnerability	Fortinet FortiWLM	✗	✗	✓

Vulnerability Timeline



Flaw discovered and disclosed to Fortinet

May 2023

End of September 2023

Patches Released

POC Disclosed

March 14, 2024

December 18, 2024

Disclosed Publicly

Vulnerability Details

#1 Fortinet has addressed an unauthenticated file read vulnerability in FortiWLM, tracked as CVE-2023-34990. If exploited, this vulnerability allows remote, unauthenticated attackers to read sensitive files on affected systems. The issue arises from a path traversal flaw that could grant unauthorized access to confidential data.

#2 FortiWLM (Fortinet Wireless Manager) is a web-based platform used to manage controllers and access points across a network, providing real-time monitoring and centralized control for wireless networks on FortiGate devices.

#3 The CVE-2023-34990 allows attackers to target the /ems/cgi-bin/ezrf_lighttpd.cgi endpoint within FortiWLM. By injecting path traversal sequences (../) into the imagename parameter, attackers can gain unauthorized access to log files stored on the system. These logs may contain administrator session IDs, which could potentially be leveraged to hijack admin sessions, escalate privileges, and compromise devices.

#4 Though the vulnerability was discovered in May 2023, Fortinet issued a patch in end of September 2023 and disclosed the flaw in December 2024, leaving a concerning gap between the initial disclosure and the release of a fix. The delayed response and the potential gaps in the advisory have raised concerns within the security community, underscoring the critical need for timely patching of high-severity vulnerabilities. As such, it is strongly recommended that FortiWLM administrators apply all relevant updates promptly to mitigate the risks posed by this flaw.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34990	FortiWLM 8.5: Versions 8.5.0 through 8.5.4 FortiWLM 8.6: Versions 8.6.0 through 8.6.5	cpe:2.3:a:fortinet:fortiwlm:*:*:*:*:*:*:*:*	CWE-23

Recommendations

Update Immediately: Update FortiWLM to the latest patched versions 8.5.5, 8.6.6, or newer. These updates specifically address the path traversal vulnerability, CVE-2023-34990. Administrators are strongly urged to upgrade without delay to safeguard systems against potential exploitation.

Monitor Admin Sessions: Regularly review logs for unusual activity, particularly suspicious access to logs or administrator session IDs.

Regularly Audit Logs: Frequently audit system logs for evidence of unauthorized access or path traversal attempts targeting the /ems/cgi-bin/ezrf_lighttpd.cgi endpoint.

Restrict Access to FortiWLM: Limit access to the FortiWLM management interface to trusted networks or specific IP ranges using firewall rules or VPNs.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	

Patch Details

Update FortiWLM to the latest patched versions 8.5.5, 8.6.6, or newer. These updates address the path traversal vulnerability, CVE-2023-34990.

Link: https://www.fortiguard.com/psirt/FG-IR-23-144

References

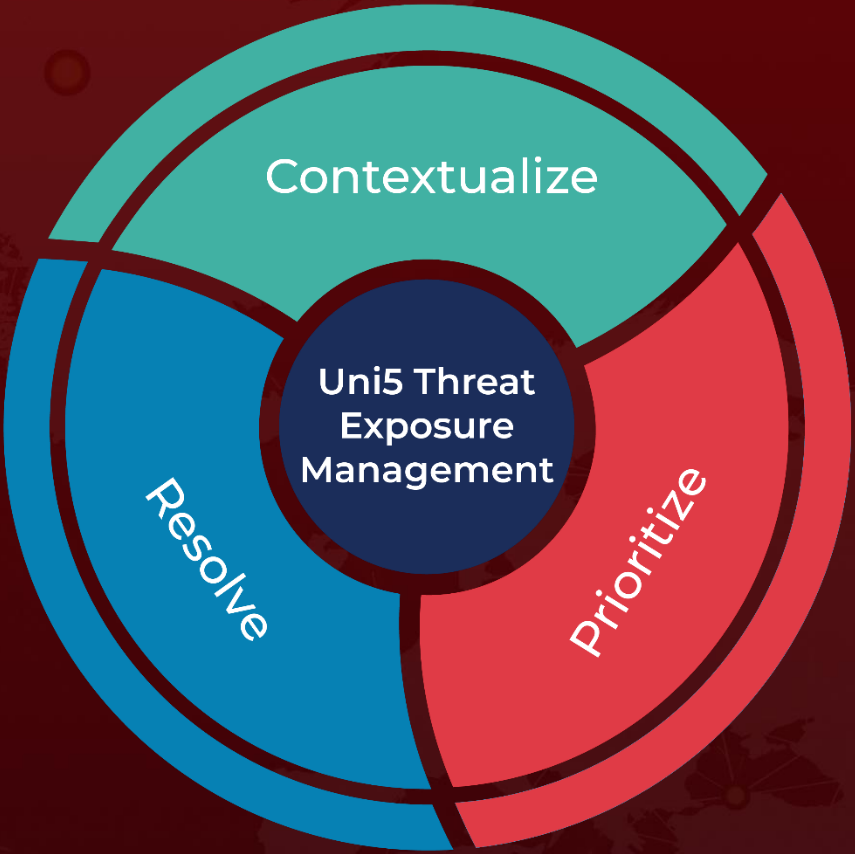
https://fortiguard.fortinet.com/psirt/FG-IR-23-144

https://www.horizon3.ai/attack-research/disclosures/fortiwlm-the-almost-story-for-the-forti-forty

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

December 20, 2024 • 5:45 AM

More at www.hivepro.com