VULNERABILITY BULLETINS

Fortinet Patches Critical FortiWLM Vulnerability CVE-2023-34990

TLP:WHITE

Dec 27, 2024

On December 18, 2024, FortiGuard Labs published a security advisory disclosing a vulnerability in FortiWLM, a wireless device management application by Fortinet. The flaw, tracked as CVE-2023-34990, has a CVSS score of 9.6, indicating its critical nature.

This vulnerability is a relative path traversal issue, which could allow remote, unauthenticated threat actors to access sensitive files. According to the National Vulnerability Database (NVD), the flaw also enables attackers to execute unauthorized code through specially crafted web requests. The NVD assigned a CVSS score of 9.8 to this vulnerability, which is higher than the score given by Fortinet.

The severity of this flaw lies in the potential for threat actors to gain access to sensitive files, such as verbose log files containing administrator session ID tokens. With these tokens, attackers could hijack sessions and gain entry to authenticated endpoints. Affected versions include 8.6.0 to 8.6.5 and 8.5.0 to 8.5.4, with fixes available in versions 8.6.6 and 8.5.5.

Health-ISAC advises urgent patching of this vulnerability if it has not already been addressed, as state-linked and financially motivated threat actors frequently target Fortinet's flaws.

Recommendations:

- Apply available patches for vulnerable Fortinet devices.
- Ensure all of the devices are patched in a timely manner.
- Enforce network segmentation and strict network access control policies.
- Continuously monitor for suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	HHS, Fortinet, Security Week, socradar, NIST-CSF

Sources
[FortiWLM] Unauthenticated Limited File Read Vulnerability
Fortinet Patches Critical FortiWLM Vulnerability
Critical Path Traversal in FortiWLM (CVE-2023-34990) Permits Code Execution
National Vulnerability Database

Release Date
Dec 27, 2024 (UTC)

Alert ID a3c54206

View Alert

Share Feedback
was this helpful? |

Tags CVE-2023-34990, Fortinet FortiWLM

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**