IMPORTANT CYBERSECURITY NEWS: OVER 12,000 KERIOCONTROL FIREWALLS EXPOSED TO EXPLOITED RCE FLAW

Vairav Cyber Security News Report

Date: 02-11-2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A critical vulnerability identified as CVE-2024-52875 has been discovered in GFI KerioControl firewalls, affecting versions 9.2.5 through 9.4.5. This flaw allows attackers to execute remote code with a single click by exploiting a CRLF injection vulnerability. Despite the release of a security patch on December 19, 2024, over 12,000 KerioControl firewall instances remain exposed to potential exploitation. Security experts strongly advise organizations to update their systems promptly to mitigate the risk.

DETAILS OF THE INCIDENT

Description: The vulnerability stems from improper sanitization of user input in specific URI paths of the KerioControl web interface, particularly the 'dest' parameter. This flaw enables attackers to perform HTTP response splitting attacks, leading to reflected cross-site scripting (XSS) and potentially allowing remote code execution. By crafting a malicious URL, an attacker can trick an authenticated administrator into executing arbitrary code, resulting in full control over the firewall system.

Identification: Security researcher Egidio Romano identified and reported the vulnerability in mid-December 2024. Following the disclosure, GFI Software released version 9.4.5 Patch 1 on December 19, 2024, to address the issue. Despite the availability of this patch, recent reports indicate that a significant number of KerioControl instances remain unpatched and vulnerable.

Affected Entities/Industries: The vulnerability impacts organizations using GFI KerioControl firewalls across various industries. Geographical data indicates that the highest concentrations of exposed instances are in Iran, the United States, Italy, Germany, and Russia.

Potential Impact:

- Complete system compromise, granting attackers root access to the firewall.
- Unauthorized access to sensitive data traversing the network.

- Potential for further attacks within the compromised network environment.

Exploitation Methods: Attackers craft malicious URLs containing CRLF sequences and specific payloads. When an authenticated administrator clicks on such a link, the server processes the injected sequences, leading to the execution of arbitrary code and granting the attacker control over the system.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- **Apply Security Patch:** Update KerioControl to version 9.4.5 Patch 1 or later to address the vulnerability.
- **Restrict Access:** Limit access to the KerioControl web management interface to trusted IP addresses.
- **Disable Public Access:** Use firewall rules to block public access to '/admin' and '/nonauth' pages.

Security Best Practices

- **User Training:** Educate administrators about the risks of clicking on unsolicited or suspicious links.
- **Regular Monitoring:** Continuously monitor network traffic for unusual activities or signs of exploitation attempts.

For Advanced Security Teams

- **Implement Web Application Firewalls (WAF):** Deploy WAFs to detect and block malicious HTTP requests targeting known vulnerabilities.
- **Conduct Regular Vulnerability Assessments:** Perform periodic security assessments to identify and remediate potential weaknesses in the network infrastructure.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/over-12-000-keriocontrol-firewalls-exposed-to-exploited-rce-flaw/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com