AL2025_10 Over 12,000 KerioControl Firewalls Exposed to Critical RCE Vulnerability (11th February 2025)

Description

A critical remote code execution (RCE) vulnerability, tracked as CVE-2024-52875, has been identified in GFI KerioControl firewalls, leaving over 12,000 instances exposed to potential exploitation. KerioControl is a widely used network security solution designed for small and medium-sized businesses, providing VPN services, bandwidth management, reporting and monitoring, traffic filtering, antivirus protection, and intrusion prevention. The vulnerability, discovered by security researcher Egidio Romano (EgiX) in mid-December 2024, allows attackers to execute arbitrary code remotely with minimal effort. Despite security updates being released, a significant number of vulnerable instances remain exposed, increasing the risk of cyberattacks.

Attack Details

The vulnerability stems from improper input validation in certain pages of the KerioControl web interface. The dest GET parameter is not adequately sanitized before being used to generate a "Location" HTTP header in a 302 HTTP response. This flaw allows attackers to perform HTTP Response Splitting attacks, which can lead to Reflected Cross-Site Scripting (XSS) and potentially enable one-click RCE attacks.

An attacker can craft a malicious URL that, when clicked by a logged-in administrator, executes arbitrary code on the firewall. This allows threat actors to compromise network security, steal credentials, and gain unauthorized access to sensitive systems. Despite the security update released in version 9.4.5 Patch 1 on December 19, 2024, thousands of instances remained vulnerable well into January 2025. Active exploitation attempts leveraging the public proof-of-concept (PoC) exploit were first observed by Greynoise early last month. More recently, The Shadowserver Foundation has detected 12,229 exposed KerioControl firewalls being targeted by cybercriminals.

Indicators of Compromise (IOCs)

Security researchers and monitoring services have identified the following IOCs related to attacks leveraging CVE-2024-52875:

- **Suspicious HTTP requests** containing crafted "dest" GET parameters
- **Unexpected administrator session hijacking** or unauthorized configuration changes
- **Presence of foreign IP addresses** in KerioControl admin login logs
- **Malicious payload execution** leading to system crashes or unauthorized access
- **Network traffic anomalies** indicating command-and-control (C2) communication

Remediation

To mitigate the risk associated with CVE-2024-52875, organizations using KerioControl must take immediate action:

1. **Update to the latest version**: Install **KerioControl 9.4.5 Patch 2**, released on **January 31, 2025**, which includes additional security enhancements.

2. **Apply access restrictions**: Limit administrative access to trusted IP addresses only.
3. **Enable Web Application Firewall (WAF)**: Use WAF rules to detect and block malicious HTTP requests.
4. **Monitor logs and network activity**: Regularly review logs for unauthorized access attempts and anomalies.
5. **Educate administrators**: Warn IT staff about phishing tactics that exploit this vulnerability.
6. **Disable remote management if unnecessary**: Restrict external access to the management interface.

Organizations that have yet to apply the security patch remain at high risk of exploitation. Immediate action is crucial to safeguard systems from potential attacks leveraging CVE-2024-52875. The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Rolf, J. (2025, January 8). January 7 Advisory: GFI KerioControl Susceptible to 1-Click RCE vulnerability [CVE-2024-52875] | Retrieved from Censys. Censys. https://censys.com/cve-2024-52875/
- Toulas, B. (2025, February 10). Over 12,000 KerioControl firewalls exposed to exploited RCE flaw. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/over-12-000-keriocontrol-firewalls-exposed-to-exploited-rce-flaw/