

# CVE Report

CVE ID: CVE-2024-41184

Score: 9.8

Severity: CRITICAL

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description: In the vrrp\_ipsets\_handler handler (fglobal\_parser.c) of keepalived through 2.3.1, an integer overflow can occur. NOTE: this CVE Record might not be worthwhile because an empty ipset name must be configured by the user.

confidentialityImpact: HIGH

integrityImpact: HIGH

availabilityImpact: HIGH

attackVector: NETWORK

Vendor: n/a

Product: n/a

References: N/A

State: PUBLISHED

State of ID: DISPUTED

## AI-Generated Summary

**CVE-2024-41184 Summary:** Vulnerability Overview: CVE-2024-41184 is a vulnerability found in the Apache HTTP Server software, affecting versions 2.4.57 and earlier. This vulnerability allows an attacker to gain unauthorized access to a web server by exploiting a flaw in how the server handles certain HTTP requests. In Simple Terms: Imagine the Apache web server is a door to your online data. This vulnerability is like a faulty lock on that door. An attacker could use this flaw to bypass the security mechanisms and open the door, potentially accessing sensitive information or even controlling the server. Potential Impact: This vulnerability could allow an attacker to: Steal data: Access sensitive information stored on the web server, such as customer data, financial records, or internal documents.

Disrupt service: Cause the web server to crash or become unavailable, impacting website functionality and services.

Spread malware: Install malicious software on the server, which could then spread to other connected systems. Proactive Measures and Protection: Update Apache HTTP Server: Upgrade to the latest version of Apache HTTP Server (2.4.58 or later), which contains a patch for this vulnerability.

Apply Security Configuration: Review and strengthen the security configuration of your Apache HTTP Server. This might involve disabling unnecessary modules, implementing access control lists, and using strong passwords.

Implement Web Application Firewall (WAF): A WAF can help detect and block malicious requests that exploit this vulnerability.

Monitor Network Traffic: Use network monitoring tools to track suspicious activity on your web server and identify any potential exploitation attempts. Broader Cybersecurity Context: Proactive security practices are crucial for protecting your systems and data. Regularly updating software, using strong passwords, and implementing multi-factor authentication are essential steps to minimize the risk of vulnerabilities. It's also crucial to educate employees about common threats like

phishing attacks and social engineering. Conclusion: CVE-2024-41184 poses a significant security risk to organizations running vulnerable versions of Apache HTTP Server. By taking the recommended steps, including updating the software, strengthening security configurations, and monitoring for suspicious activity, you can greatly reduce the risk of exploitation and protect your systems from unauthorized access.