CRITICAL SSL FortiGate VPN VULNERABILITY

Analysis and Mitigation Strategies

An Overview of CVE-2023-27997 and Key Mitigation Steps

Research by: Galih Samoeri
Date: February 2025

ABSTRACT

Background: In June 2023, a critical vulnerability (CVE-2023-27997) was discovered in FortiGate's SSL VPN, allowing threat actors to bypass authentication and perform arbitrary code execution on affected systems. With a CVSS score of 9.8 (Critical), this vulnerability has been actively exploited by advanced threat actors targeting government agencies, financial institutions, and large enterprises. This report provides detailed analysis of the vulnerability, its real world impact and actionable mitigation strategies to help organisations defend against this threat.

INTRODUCTION

In June 2023, a critical vulnerability (CVE-2023-27997) was discovered in FortiGate's SSL VPN, a widely used VPN solution for secure remote access. This weakness allows attackers to bypass authentication and execute malicious code on affected machines. With an objectively high CVSS score of 9.8 (Critical), this vulnerability poses significant risks to organisations utilising FortiGate's VPN.

TECHNICAL BREAKDOWN

- **CVE ID:** CVE-2023-27997
- **Severity:** CVSS 9.8 (Critical)
- **Affected Systems:** FortiOS versions 6.0.0 to 6.0.15, 6.2.0 to 6.2.14, and 6.4.0 to 6.4.11
- **Attack Type:** Authentication Bypass → Remote Code Execution (RCE)
- **How It Works:** Attackers exploit a **heap-based buffer overflow** in the SSL VPN component. This vulnerability lets them bypass login screens and execute malicious code on vulnerable systems, potentially gaining full control of the device.

REAL-WORLD EXPLOITATION

This vulnerability has been targeted by sophisticated threat actors, including nation-state actors and ransomware groups. It has affected high-profile targets such as government agencies, financial institutions, and large enterprises. These attackers have used the vulnerability as an entry point to deliver payloads, gain access to sensitive data, and deploy malware.

MITRE ATT&CK FRAMEWORK MAPPING

Tactics:

- **Initial Access (TA0001):** Attackers gain access through the vulnerability and bypass authentication mechanisms.
- **Privilege Escalation (TA0004):** Once inside, they may exploit the vulnerability to escalate privileges and take full control of the system.

Techniques:

- **Exploitation of Public Facing Application (T1190):** The vulnerability affects publicly accessible systems, such as VPNs exposed to the internet.
- **Remote Code Execution (RCE) (T1203):** Once the attacker has bypassed authentication, they can execute arbitrary code remotely.

MITIGATION STRATEGIES

---

1. **Patch Immediately**: This is the most crucial and critical step. Ensure systems are updated with the latest FortiOS versions to close the vulnerability.
2. **Restrict Access**: Limiting access to VPN services based on trusted IP addresses can reduce the exposure of your systems. For added security, use firewall rules to block any unauthorized traffic.
3. **Enable Multi-Factor Authentication (MFA)**: Adding MFA ensures that even if an attacker bypasses authentication, they will still need a second form of verification to access the system.
4. **Monitor for Anomalies**: Regular monitoring with SIEM tools can help detect any suspicious behavior, such as failed login attempts or unusual traffic. This can help you identify and mitigate any attacks early.
5. **Conduct Penetration Testing and Vulnerability Scanning**: Regularly test systems to uncover other potential weaknesses and vulnerabilities. Vulnerability scanners can efficiently help identify outdated software versions and unpatched systems that are still vulnerable.

CONCLUSION

CVE-2023-27997 poses a significant risk to organisations that rely on FortiGate's SSL VPN for remote access. It's crucial to patch the systems immediately, but also to implement strong access controls, enable multi-factor authentication, and use monitoring tools to detect and respond to suspicious activity. Staying proactive with these mitigations will help protect against this and future threats.