IMPORTANT CYBERSECURITY NEWS: NEW SUPERBLACK RANSOMWARE EXPLOITS FORTINET AUTH BYPASS FLAWS

Vairav Cyber Security News Report

Date: March 14th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A new ransomware variant named ‘SuperBlack’ has emerged, targeting organizations by exploiting critical authentication bypass vulnerabilities in Fortinet’s security appliances. Attackers, identified as the ‘Mora_001’ group, have leveraged CVE-2024-55591 and CVE-2025-24472 to gain unauthorized access to FortiGate firewalls, leading to data encryption and operational disruptions. This development underscores the imperative for organizations to promptly apply security patches and reinforce their network defenses.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The ‘SuperBlack’ ransomware campaign exploits two critical vulnerabilities in Fortinet’s FortiOS and FortiProxy products:

- **CVE-2024-55591**: An authentication bypass vulnerability that allows unauthenticated attackers to gain super-admin privileges by sending crafted requests to the Node.js websocket module.
- **CVE-2025-24472**: Another authentication bypass flaw enabling attackers to achieve super-admin access through specially crafted CSF proxy requests.

Notably, SuperBlack is a customized variant of the LockBit 3.0 ransomware builder, indicating potential ties to the LockBit group.

Identification: The campaign was identified in late January 2025 when Forescout’s Vedere Labs detected unauthorized activities linked to the exploitation of Fortinet vulnerabilities. Subsequent analysis confirmed the deployment of the SuperBlack ransomware.

Threat Actor: The group ‘Mora_001’ is attributed to these attacks. While their exact affiliation remains uncertain, the use of a customized LockBit 3.0 builder suggests possible connections to the LockBit ransomware group.

Affected Entities/Industries: Organizations utilizing unpatched Fortinet FortiGate firewalls and FortiProxy appliances are at risk. The campaign appears opportunistic, targeting entities with exposed and vulnerable Fortinet devices.

Potential Impact:

- **Financial Losses**: Costs associated with ransom payments, system restoration, and potential regulatory fines.
- **Operational Downtime**: Disruption of critical services during system encryption and recovery phases.
- **Data Exposure**: Risk of sensitive information being exfiltrated and potentially leaked.
- **Reputational Damage**: Loss of trust among clients and partners due to security breaches.

Exploitation Methods: Attackers exploited the identified Fortinet vulnerabilities to gain initial access. Post-compromise, they utilized tools like Windows Management Instrumentation (WMIC) for system discovery and lateral movement, and Secure Shell (SSH) for accessing additional systems. A custom data exfiltration tool unique to SuperBlack was deployed prior to encryption, followed by a wiper tool to remove traces of the ransomware executable.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply the latest security patches for FortiOS and FortiProxy to address CVE-2024-55591 and CVE-2025-24472.
- Disable external management access to firewalls and VPNs where possible.
- Conduct a thorough audit of administrative accounts to identify and remove unauthorized users.

Security Best Practices

- Regularly update all software and firmware to their latest versions.
- Implement network segmentation to limit lateral movement opportunities for attackers.
- Enforce multi-factor authentication (MFA) for all remote access points.

- Maintain up-to-date offline backups of critical data.

For Advanced Security Teams

- Monitor network traffic for anomalies indicative of exploitation attempts.
- Utilize intrusion detection and prevention systems (IDPS) to identify and block malicious activities.
- Engage in threat hunting exercises focusing on the tactics, techniques, and procedures (TTPs) associated with the SuperBlack ransomware.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/new-superblack-ransomware-exploits-fortinet-auth-bypass-flaws/
- https://www.computerweekly.com/news/366620584/SuperBlack-ransomware-may-have-ties-to-LockBit
- https://www.scworld.com/news/new-lockbit-linked-ransomware-group-targets-fortinet-vulnerabilities

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: sales@vairavtech.com

Website: https://vairavtech.com