EnCyb

Severity: High

Advisory Type: Threat

FortiWeb Sliver C2 Compromise

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Attackers exploited outdated FortiWeb appliances to deploy the Sliver C2 framework, gaining persistent, stealthy access to network perimeters. The campaign highlights a critical visibility gap in edge devices and underscores the need for urgent patching and enhanced monitoring of internet-facing security appliances.

- **Active Region:** Asia
- **Affected Sector:** Government, Financial Services, Enterprises
- **Affected Product:** Fortinet FortiWeb Web Application Firewall
- **Severity:** High
- **Published Date:** January 05, 2026

TECHNICAL DETAILS

- **Target:** Internet-facing Fortinet FortiWeb Web Application Firewall appliances, particularly those deployed at network perimeters and protecting critical web applications in government and financial environments.
- **Root Cause**: Use of outdated FortiWeb firmware with exploitable public-facing vulnerabilities (including CVE-2025-55182), combined with limited security visibility and lack of endpoint monitoring on edge appliances.
- **Prerequistic For Exploitation:** Internet-exposed FortiWeb appliances running unpatched firmware versions 5.4.202–6.1.62 with limited monitoring and security controls.

IOC

IOC Type	Value
Domain	ns1.ubunutpackages[.]store
Domain	ns1.bafairforce[.]army
Domain	testing.caai[.]in
IP Address	195.20.17[.]253
IP Address	193.233.201[.]12

IP Address	45.150.108[.]43
IP Address	80.78.18[.]142
IP Address	192.81.210[.]81
IP Address	45.143.167[.]7
IP Address	45.83.181[.]160
File Hash (SHA-256)	4086057b9a0f9898c07318e093814ae9cfdaaf6ad71a45b2d0d4cd75e57f9354
File Hash (SHA-256)	964473ffbd593fc52a779b1d699c79cc66b459cf842c2e6221703e2e6a2322c0
File Hash (SHA-256)	172a9ee9601ef0eb6fbd2676742edfb201c10369712dbf721e5d105aa1320a32
File Hash (SHA-256)	3c24f30f2ca89d408d42293cab8fbb81cb9c2b0801074ef40f0a79770dac5956
File Hash (SHA-256)	2897ee24de4cca2a4c6a085cf6fdccb6a89c6c23978529d81b4f4e6db46b0b96
File Hash (SHA-256)	dafc7517669e931de858464966af995c44c2e7c6bdf684d53c54d6503cd48a38

IMPACT

- Unauthorized remote access to affected systems
- Persistent attacker access to perimeter security appliances
- Covert command-and-control and proxy infrastructure within trusted networks
- Increased risk of lateral movement into internal systems
- Potential exposure or manipulation of sensitive application traffic

RECOMMENDATIONS

- Disable or strictly restrict macro-enabled Office documents
- Immediately patch or upgrade FortiWeb appliances to the latest supported firmware versions
- Restrict internet exposure of FortiWeb management interfaces and enforce strong access controls
- Apply strict egress filtering to limit outbound connections from perimeter devices
- Regularly audit appliance configurations, startup services, and file systems for unauthorized changes
- Enforce network segmentation to prevent lateral movement from compromised perimeter systems
- Incorporate edge devices into vulnerability management and threat-hunting programs

REFRENCE

- https://cyberpress.org/fortiweb-sliver-c2-attack/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com