INTRUVENT

VULNERABILITY ADVISORY

CVE-2024-21762

FortiOS SSL VPN Out-of-Bounds Write - Pre-Authentication RCE

CVSS Score 9.8 (Critical)
Published 2025-12-06
Classification TLP:CLEAR
Exploitation Active ITW - PoC Public

Intruvent Technologies

INT-VA-2025-CVE-2024-21762-v1.0

1 Executive Summary

9.8 **Critical Severity**
Out-of-Bounds Write / Pre-Auth RCE - CWE-787
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Pre-Authentication Remote Code Execution
CVE-2024-21762 allows unauthenticated attackers to execute arbitrary code on FortiGate devices with SSL VPN enabled. A public proof-of-concept exploit has been available since March 2024. Approximately 150,000 vulnerable devices remain exposed according to Shadowserver Foundation. Chinese state-sponsored threat actor Volt Typhoon has been linked to exploitation of this vulnerability.

CVE-2024-21762 is an out-of-bounds write vulnerability in the FortiOS SSL VPN daemon (`sslvpnd`). The flaw exists in the HTTP chunked transfer encoding parser. By sending specially crafted HTTP requests with manipulated chunk trailers, an unauthenticated attacker can trigger a stack-based buffer overflow, ultimately achieving remote code execution on the device.

Key Facts

CVE ID	CVE-2024-21762
Vendor Advisory	FG-IR-24-015
CVSS v3.1	9.8 (Critical)
CWE	CWE-787: Out-of-Bounds Write
Attack Vector	Network (Remote, No Authentication)
Vulnerable Component	sslvpnd (SSL VPN daemon)
Exploitation	Active in-the-wild; PoC public since March 2024
CISA KEV	Added February 2024
Exposed Devices	~150,000 (Shadowserver)
Threat Actors	Volt Typhoon (Chinese state-sponsored), Qilin ransomware

2 Affected Products

FortiOS Affected Versions

Version Branch	Vulnerable Versions	Fixed Version
FortiOS 7.4	7.4.0 - 7.4.2	**7.4.3+**
FortiOS 7.2	7.2.0 - 7.2.6	**7.2.7+**
FortiOS 7.0	7.0.0 - 7.0.13	**7.0.14+**
FortiOS 6.4	6.4.0 - 6.4.14	**6.4.15+**
FortiOS 6.2	6.2.0 - 6.2.15	**6.2.16+**
FortiOS 6.0	6.0.x (all versions)	**Migrate to fixed release**

FortiProxy Affected Versions

Version Branch	Vulnerable Versions	Fixed Version
FortiProxy 7.4	7.4.0 - 7.4.2	**7.4.3+**
FortiProxy 7.2	7.2.0 - 7.2.8	**7.2.9+**
FortiProxy 7.0	7.0.0 - 7.0.14	**7.0.15+**
FortiProxy 2.0	2.0.0 - 2.0.13	**2.0.14+**
FortiProxy 1.x	1.0.x - 1.2.x (all versions)	**Migrate to fixed release**

Prerequisite for Exploitation
This vulnerability affects devices with **SSL VPN enabled**. Devices without SSL VPN functionality enabled are not vulnerable. However, given the prevalence of SSL VPN usage, most FortiGate deployments are likely affected.

3 Technical Analysis

Vulnerability Mechanism

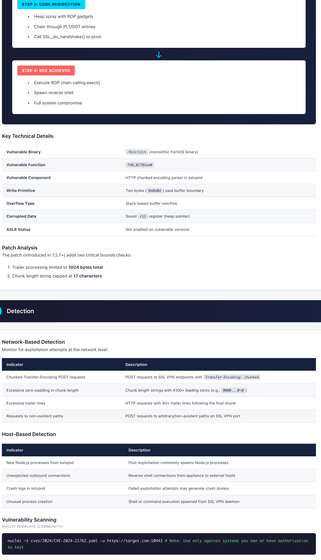
The vulnerability exists in the HTTP chunked transfer encoding parser within `sslvpnd`, the SSL VPN daemon. The flaw is in function **`FUN_81781ce0`** which processes HTTP trailers following chunked data.

Root Cause
When processing HTTP trailers after a zero-length final chunk, the vulnerable code writes carriage return and line feed characters (`0x0d0a`) beyond the allocated buffer without proper bounds checking. The offset used for writing increments with each trailer encountered but is never validated against the remaining buffer space.

```
// Simplified vulnerable logic */ offset = 0; for (each trailer in request) { buffer[offset] = 0x0d; // Carriage return buffer[offset+1] = 0x0a; // Line feed offset += 2; // NO CHECK: offset > buffer_size } // Result: Stack overflow with limited data (0x0d0a only)
```

Exploitation Chain

Despite only being able to write two bytes (`0x0d0a`) past the buffer, researchers at Assetnote demonstrated this is sufficient for reliable RCE:



Key Technical Details

Vulnerable Binary	`/bin/sslvpnd` (monolithic FortiOS binary)
Vulnerable Function	**`FUN_81781ce0`**
Vulnerable Component	HTTP chunked encoding parser in sslvpnd
Write Primitive	Two bytes (`0x0d0a`) past buffer boundary
Overflow Type	Stack-based buffer overflow
Corrupted Data	Saved `r13` register (heap pointer)
ASLR Status	Not enabled on vulnerable versions

Patch Analysis

The patch (introduced in 7.2.7+) adds two critical bounds checks:

1. Trailer processing limited to **1024 bytes total**
2. Chunk length string capped at **17 characters**

4 Detection

Network-Based Detection

Monitor for exploitation attempts at the network level:

Indicator	Description
Chunked Transfer-Encoding POST requests	POST requests to SSL VPN endpoints with `Transfer-Encoding: chunked`
Excessive zero-padding in chunk length	Chunk length strings with 4100+ leading zeros (e.g., `0000...0FA0`)
Excessive trailer lines	HTTP requests with 80+ trailer lines following the final chunk
Requests to non-existent paths	POST requests to arbitrary/non-existent paths on SSL VPN port

Host-Based Detection

Indicator	Description
New Node.js processes from sslvpnd	Post-exploitation commonly spawns Node.js processes
Unexpected outbound connections	Reverse shell connections from appliance to external hosts
Crash logs in sslvpnd	Failed exploitation attempts may generate crash dumps
Unusual process creation	Shell or command execution spawned from SSL VPN daemon

Vulnerability Scanning

Nuclei template (community):

```
nuclei -t cves/2024/CVE-2024-21762.yaml -u https://target.com:10443 # Note: Use only against systems you own or have authorization to test
```

IOC Limitations
Researchers note that "not much has been released in terms of IOCs for this vulnerability." Focus on behavioral detection (unusual processes from sslvpnd) rather than static indicators.

5 Remediation

PATCH IMMEDIATELY Pre-auth RCE - PoC public - 150K+ exposed devices

Patching Guidance

Apply the appropriate patch for your FortiOS/FortiProxy version:

Product	Current Version	Upgrade To
FortiOS 7.4	7.4.0 - 7.4.2	**7.4.3+**
FortiOS 7.2	7.2.0 - 7.2.6	**7.2.7+**
FortiOS 7.0	7.0.0 - 7.0.13	**7.0.14+**
FortiOS 6.4	6.4.0 - 6.4.14	**6.4.15+**
FortiOS 6.2	6.2.0 - 6.2.15	**6.2.16+**
FortiOS 6.0	All versions	**Migrate to supported version**
FortiProxy 7.4	7.4.0 - 7.4.2	**7.4.3+**
FortiProxy 7.2	7.2.0 - 7.2.8	**7.2.9+**
FortiProxy 7.0	7.0.0 - 7.0.14	**7.0.15+**
FortiProxy 2.0	2.0.0 - 2.0.13	**2.0.14+**

Temporary Workaround

If immediate patching is not possible, **disable SSL VPN functionality**:

Disable SSL VPN

```
config vpn ssl settings set status disable end
```

Critical Warning
Fortinet's advisory explicitly states that **disabling webmode is NOT a valid workaround**. The vulnerability exists in the core SSL VPN daemon, not just the web interface. The only effective workarounds are:

- Apply patches
- Completely disable SSL VPN

Post-Compromise Actions

If exploitation is suspected:

1. **Isolate the device** - Disconnect from network if possible
2. **Forensic imaging** - Capture memory and disk for analysis
3. **Review process list** - Check for unusual processes spawned from sslvpnd
4. **Review network connections** - Identify reverse shells or C2 traffic
5. **Assume breach** - Investigate lateral movement into internal network
6. **Rebuild device** - Do not trust patching alone after confirmed compromise

6 Threat Actor Context

Volt Typhoon

Fortinet has disclosed that **Volt Typhoon**, a Chinese state-sponsored threat actor, has been targeting FortiOS vulnerabilities to deploy custom malware. Volt Typhoon is known for:

- Living-off-the-land techniques for persistence
- Targeting critical infrastructure (energy, water, telecommunications)
- Pre-positioning for potential disruptive operations
- Extended dwell times with minimal detection

Ransomware Affiliates

Qilin ransomware affiliates have been observed exploiting CVE-2024-21762 for initial access to enterprise networks. After exploiting FortiGate devices, they proceed with:

- Credential harvesting from Veeam backups
- Lateral movement via RDP and admin shares
- Chrome credential theft via DPD
- Data exfiltration before encryption

Internet Exposure
According to the Shadowserver Foundation, approximately **150,000 devices** remain vulnerable to CVE-2024-21762. Organizations should prioritize patching any internet-exposed FortiGate devices.

7 References

Fortinet PSIRT Advisory FG-IR-24-015

Assetnote - Two Bytes Is Plenty: FortiGate RCE with CVE-2024-21762

Tenable - CVE-2024-21762 Analysis

CISA Known Exploited Vulnerabilities Catalog

BleepingComputer - Fortinet RCE Flaw Coverage

SOCRadar - FortiOS SSL VPN RCE Analysis

NHS England Digital - CVE-2024-21762 Advisory