INTRUVENT

VULNERABILITY ADVISORY

CVE-2024-55591

FortiOS & FortiProxy Authentication Bypass via Node.js WebSocket

CVSS Score 9.6 (Critical)
Classification TLP:CLEAR
Published 2025-12-06
Exploitation Active Zero-Day (Nov 2024+)

Intruvent Technologies
INT-VA-2025-CVE-2024-55591-v1.0

1 Executive Summary

9.6

Critical Severity
Authentication Bypass - CWE-288
`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Active Zero-Day Exploitation
CVE-2024-55591 has been actively exploited since mid-November 2024, weeks before public disclosure. Threat actors are gaining super-admin privileges on FortiGate firewalls, creating rogue accounts, and using SSL VPN to tunnel into enterprise networks. CISA added this to the KEV catalog on January 17, 2025.

CVE-2024-55591 is an authentication bypass vulnerability in Fortinet FortiOS and FortiProxy. A remote, unauthenticated attacker can send specially crafted requests to the Node.js websocket module to gain **super-admin privileges** on vulnerable devices. This allows complete control over the firewall, including creating admin accounts, modifying policies, and enabling VPN access for lateral movement into internal networks.

Key Facts

CVE ID	CVE-2024-55591
Vendor Advisory	FG-IR-24-535
CVSS v3.1	9.6 (Critical)
CWE	CWE-288: Authentication Bypass Using an Alternate Path or Channel
Attack Vector	Network (Remote, No Authentication)
Exploitation	Active zero-day since November 2024
CISA KEV	Added January 17, 2025
Ransomware Use	Qilin affiliates observed using for initial access

2 Affected Products

Vulnerable Versions

Product	Vulnerable Versions	Fixed Version
FortiOS	7.0.0 through 7.0.16	**7.0.17 or above**
FortiProxy	7.0.0 through 7.0.19	**7.0.20 or above**
FortiProxy	7.2.0 through 7.2.12	**7.2.13 or above**

Not Affected
The following versions are NOT vulnerable:

- FortiOS 7.6.x, 7.4.x, 7.2.x, 6.4.x
- FortiProxy 7.6.x, 7.4.x, 2.0.x

Related Vulnerability

CVE-2025-24472 (CVSS 8.1) - A related authentication bypass via CSF proxy requests was disclosed on February 11, 2025. The same patches address both vulnerabilities.

3 Technical Analysis

Vulnerability Description

The vulnerability exists in the Node.js websocket module used by the FortiOS/FortiProxy web management interface. By sending specially crafted requests to this module, an unauthenticated attacker can bypass authentication and gain **super-admin** privileges on the device.

Attack Vector

Exploitation requires only network access to the management interface (typically HTTPS on port 443 or a custom admin port). No authentication or user interaction is required. The attack is executed via the `jsconsole` interface, which is normally used for CLI commands through the web GUI.

Impact

Successful exploitation grants the attacker complete control over the firewall:

- **Create Admin Accounts:** Add new super-admin users with randomly generated names
- **Create Local Users:** Add local users to SSL VPN groups
- **Modify Firewall Policies:** Change security rules to allow unauthorized access
- **Access SSL VPN:** Tunnel into internal networks via newly created VPN accounts
- **Credential Harvesting:** Extract credentials for lateral movement

4 Exploitation Timeline

Arctic Wolf documented a coordinated attack campaign exploiting this vulnerability before public disclosure:

Date Range	Phase	Activity
Nov 16–23, 2024	Scanning	Automated vulnerability scanning of internet-exposed FortiGate devices
Nov 22–27, 2024	Reconnaissance	Configuration enumeration and changes via jsconsole
Dec 4–7, 2024	Privilege Escalation	Creation of super-admin accounts with random usernames; hijacking of existing accounts
Dec 16–27, 2024	Lateral Movement	Credential extraction; SSL VPN tunneling into internal networks
Jan 10, 2025	Public Disclosure	Arctic Wolf publishes campaign analysis
Jan 14, 2025	Vendor Advisory	Fortinet releases advisory FG-IR-24-535
Jan 17, 2025	CISA KEV	Added to Known Exploited Vulnerabilities catalog

5 Detection

Indicators of Compromise

Log Patterns
Monitor FortiGate logs for suspicious jsconsole activity with spoofed source/destination IPs:

```
# Exploitation indicator - admin login via jsconsole with spoofed IPs type="event" subtype="system" level="information" logdesc="Admin login successful" user="LOCAL_Process_Access" # Alternative pattern - note srcip/dstip values are attacker-controlled ui="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success"
```

Important Note
The `srcip` and `dstip` values in exploitation logs are attacker-controlled and spoofed. Do not rely on these IPs for attribution - they are arbitrary values provided by the attacker.

Behavioral Indicators

Indicator	Detection Method
Unauthorized admin account creation	Monitor for new admin accounts with random/unusual usernames
Local user creation	Alert on new local users, especially those added to SSL VPN groups
Firewall policy changes	Audit configuration changes originating from jsconsole interface
SSL VPN tunnel creation	Monitor for VPN connections from newly created accounts
Unexpected jsconsole logins	Alert on jsconsole authentication events outside normal admin activity

Compromise Assessment Queries

FORTIGATE CLI: CHECK FOR UNAUTHORIZED ADMIN ACCOUNTS

```
diagnose sys admin list # Review for unexpected admin accounts config system admin show # Audit all admin accounts and their creation dates
```

FORTIGATE CLI: REVIEW RECENT CONFIGURATION CHANGES

```
diagnose debug config-error-log read # Check for configuration changes execute log filter category event execute log filter subtype system execute log display # Review system events for unauthorized activity
```

6 Remediation

PATCH IMMEDIATELY Active zero-day exploitation - CISA KEV listed

Patching Guidance

Product	Current Version	Upgrade To
FortiOS	7.0.0 - 7.0.16	**7.0.17 or above**
FortiProxy	7.0.0 - 7.0.19	**7.0.20 or above**
FortiProxy	7.2.0 - 7.2.12	**7.2.13 or above**

Temporary Workarounds

If immediate patching is not possible:

OPTION 1: DISABLE HTTP/HTTPS ADMINISTRATIVE INTERFACE

```
config system interface edit "port1" # or your management interface set allowaccess ping https ssh unset allowaccess http https # Disable web management next end
```

OPTION 2: RESTRICT MANAGEMENT ACCESS VIA LOCAL-IN POLICY

```
config firewall local-in-policy edit 1 set intf "port1" # Management interface set srcaddr "Trusted_Admin_IPs" # Address object for allowed IPs set dstaddr "all" set action accept set service HTTPS SSH set schedule "always" next edit 2 set intf "port1" set srcaddr "all" set dstaddr "all" set action deny set service HTTPS HTTP set schedule "always" next end
```

Post-Compromise Actions

If exploitation is suspected or confirmed:

1. **Audit all admin accounts** - Remove any unauthorized accounts immediately
2. **Audit local users** - Check for users added to SSL VPN groups
3. **Review firewall policies** - Identify and revert unauthorized changes
4. **Reset all admin credentials** - Change passwords for all legitimate admin accounts
5. **Review VPN logs** - Identify any unauthorized VPN tunnels
6. **Forensic investigation** - Assess lateral movement into internal network

7 References

Fortinet PSIRT Advisory FG-IR-24-535

Arctic Wolf - CVE-2024-55591 Campaign Analysis

Tenable - CVE-2024-55591 Analysis

CISA Known Exploited Vulnerabilities Catalog

Help Net Security - Fortinet Zero-Day Coverage