INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 19:09 UTC

Gentlemen Ransomware Group Exploits CVE-2024-55591 Fortinet Auth Bypass with AI-Assisted TTPs

THREAT CAMPAIGN | **HIGH** | CVSS 9.6

SCC Item ID	SCC-CAM-2026-0401
Type	Threat Campaign
CVE ID	CVE-2024-55591
Severity	HIGH
CVSS Base Score	9.6
EPSS Score	0.9412 (100th percentile)
Affected Products	Fortinet FortiOS and FortiProxy, FortiOS 7.0.0-7.0.16 and FortiProxy 7.0.0-7.0.19, 7.2.0-7.2.12 (per FortiGuard Labs FG-IR-24-535)
Published	2026-06-03
Discovery Source	Gemini

Executive Summary

The Gentlemen ransomware group is actively exploiting CVE-2024-55591, a critical authentication bypass flaw (CVSS 9.6) in Fortinet FortiOS and FortiProxy, to gain super-admin access to edge devices without credentials. Organizations running unpatched FortiGate firewalls or FortiProxy appliances with management interfaces exposed to the internet face immediate ransomware deployment risk. The group has operationalized AI tools to accelerate attack development, signaling a capability escalation that shortens the window between initial access and data encryption.

Technical Analysis

CVE-2024-55591 is a critical authentication bypass vulnerability (CVSS 9.6, CWE-288, CWE-306) in Fortinet FortiOS and FortiProxy, rooted in a flaw within the Node.js websocket module used by the management interface. Affected versions: FortiOS 7.0.0-7.0.16 and FortiProxy 7.0.0-7.0.19, 7.2.0-7.2.12, per FortiGuard Labs advisory FG-IR-24-535. Exploitation allows an unauthenticated remote attacker to obtain super-admin privileges on FortiGate edge devices by sending crafted websocket requests to the management interface. The Gentlemen group combines this initial access vector (T1190) with brute-force attacks against Fortinet VPNs (T1110, T1133) and deploys custom command-and-control tooling post-access (T1059, T1041). Valid account abuse follows privilege escalation (T1078). The group additionally uses phishing lures generated with AI

assistance (T1566) and acquires tooling via open sources (T1588.002) before encrypting data (T1486). A public proof-of-concept is available in the watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-55591 GitHub repository (T3 source). CVE-2024-55591 was added to the CISA Known Exploited Vulnerabilities catalog in January 2025 and was exploited in the wild prior to patch availability. EPSS score is 0.941, placing this in the 99.9th percentile of exploitation likelihood. NVD record: https://nvd.nist.gov/vuln/detail/cve-2024-55591 (T1 source, verified). FortiGuard advisory: https://www.fortiguard.com/psirt/FG-IR-24-535 (vendor advisory, recommend human validation for current patch guidance).

Action Checklist

1. Step 1: Containment, Immediately restrict or disable internet-facing access to the FortiOS and FortiProxy management interfaces on all affected appliances (FortiOS 7.0.0-7.0.16, FortiProxy 7.0.0-7.0.19 and 7.2.0-7.2.12). Per FortiGuard FG-IR-24-535, if patching is not immediately possible, disable HTTP/HTTPS administrative access from untrusted networks as a temporary measure. Confirm firewall ACLs block external access to management ports. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query firewall and VPN logs for anomalous websocket connections to the FortiOS management interface, unexpected super-admin account creation or privilege changes, and repeated failed authentication attempts against Fortinet VPN endpoints (T1110 brute-force pattern). Review AU-2 event logging output for admin session initiations lacking corresponding MFA events. Check for new or unrecognized administrator accounts against your approved inventory (CIS 5.1, Establish and Maintain an Inventory of Accounts). Hunt for outbound connections to unknown IPs that may indicate custom C2 activity (T1041). Cross-reference any identified IPs and hashes against CISA KEV and threat feeds.
3. Step 3: Eradication, Apply FortiGuard-issued patches per FG-IR-24-535 to upgrade FortiOS to a fixed version above 7.0.16 and FortiProxy to a fixed version above 7.0.19 / 7.2.12. Rotate all administrative credentials on affected devices immediately following patching (D3FEND: D3-CRO, Credential Rotation). Audit all administrator accounts created or modified during the exposure window and remove unauthorized accounts (D3FEND: D3-LAM, Local Account Monitoring; NIST AC-2, Account Management; CIS 5.3, Disable Dormant Accounts). Review and revoke any API tokens or VPN credentials that may have been compromised.
4. Step 4: Recovery, After patching, validate that management interfaces are no longer accessible from untrusted networks. Confirm MFA is enforced on all administrative and VPN access paths (D3FEND: D3-MFA, Multi-factor Authentication; CIS 6.3, Require MFA for Externally-Exposed Applications; CIS 6.4, Require MFA for Remote Network Access; CIS 6.5, Require MFA for Administrative Access). Re-baseline expected network behavior and monitor for residual C2 beaconing or lateral movement. Audit log integrity to confirm no tampering occurred during the intrusion window (NIST AU-9, Protection of Audit Information).
5. Step 5: Post-Incident, Conduct a lessons-learned review covering: management interface exposure policies (NIST AC-17), patch cadence gaps against CISA KEV obligations (CIS 7.3, Automated OS Patch Management), and VPN authentication strength (CIS 6.4). Evaluate whether AI-assisted phishing lures (T1566) reached internal users and assess security awareness training coverage. Document control gaps and update the vulnerability management process (CIS 7.1, Establish and Maintain a Vulnerability Management Process). Consider adding FortiGate management interface traffic to continuous monitoring scope (NIST SI-4, AU-6, Audit Record Review, Analysis, and Reporting).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if forensic review of FortiOS admin event logs confirms unauthorized super-admin account creation, configuration export, or outbound data transfer during the exposure window, as these indicators suggest successful ransomware pre-positioning by the Gentlemen group and may trigger breach notification obligations under applicable data protection regulations (e.g., GDPR 72-hour notification, HIPAA 60-day notification, or SEC 4-day material incident disclosure) depending on data types accessible through the compromised FortiProxy or FortiGate segmentation points.
Recovery Notes	After patching to FortiOS 7.0.17+ or FortiProxy 7.0.20+/7.2.13+ per FG-IR-24-535, run a full administrator account audit ('config system admin / show full-configuration') and validate every account against your authorized admin roster before restoring normal operations — any unrecognized account must be treated as a Gentlemen group backdoor until proven otherwise. Monitor FortiGate SSL-VPN authentication logs and internal east-west traffic logs for a minimum of 30 days post-recovery for T1078 (Valid Accounts) abuse patterns, as the group is known to harvest VPN credentials during the initial access phase for delayed re-entry. Continuously validate that management interface ACLs remain in place through weekly external port scans, as firewall policy changes or firmware upgrades can inadvertently re-expose management ports.
Forensic Artifacts	FortiOS System Event Logs (Log & Report > System Events, action='login' and action='cfg-change'): CVE-2024-55591 exploitation via the jsconsole websocket handler produces admin session records with no corresponding credential validation event — look for 'type=event subtype=system action=login ui=jsconsole' entries with external source IPs as the primary exploitation indicator per FG-IR-24-535 technical analysis. | FortiOS Administrator Account Table ('config system admin / show full-configuration'): Gentlemen group actors create super-admin backdoor accounts post-exploitation; diff the current account table against your change management records to identify accounts added during the exposure window (FortiOS 7.0.0–7.0.16 or FortiProxy 7.0.0–7.0.19, 7.2.0–7.2.12). | FortiOS Configuration Backup ('execute backup config tftp'): A full configuration snapshot taken immediately after containment preserves the compromised state including any modified SSL-VPN policies, added static routes for C2 reachability, or altered authentication profiles that the threat actor may have inserted via the auth bypass to establish persistence. | Network Packet Captures on Management Interface (TCP 443/8443): Websocket upgrade requests ('Upgrade: websocket' HTTP header) to the FortiOS management daemon from external IPs during the exposure window constitute direct evidence of CVE-2024-55591 exploitation attempts; capture and preserve PCAP files from perimeter taps, upstream router NetFlow, or FortiGate's built-in packet capture ('diagnose sniffer packet') covering the incident timeframe. | SSL-VPN and FortiAuthenticator Authentication Logs: Gentlemen group uses harvested VPN credentials (T1078 — Valid Accounts) for lateral movement and ransomware staging after initial access via CVE-2024-55591; preserve all VPN session logs including source IP, username, session duration, and bytes transferred for the 30-day window preceding detection, as anomalous session volumes or off-hours logins from known-good accounts indicate credential misuse following the auth bypass.

Per-Action IR Details

Step 1: Containment — Immediately restrict or disable internet-facing access to the FortiOS and FortiProxy management interfaces on all affected appliances (FortiOS 7.0.0–7.0.16, FortiProxy 7.0.0–7.0.19 and 7.2.0–7.2.12). Per FortiGuard FG-IR-24-535, if patching is not immediately possible, disable HTTP/HTTPS administrative access from untrusted networks as a temporary measure. Confirm firewall ACLs block external access to management ports. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Run 'get system interface' and 'get firewall policy' from the FortiOS CLI to enumerate which interfaces have HTTP/HTTPS admin access enabled; immediately execute 'config system interface / edit / set allowaccess ping / end' to strip HTTP/HTTPS admin access without a full shutdown. On the upstream perimeter, apply ACL rules blocking TCP 443 and TCP 8443 to FortiGate management IPs from any source outside your defined admin CIDR. Verify with a port scan from an external vantage point using 'nmap -p 443,8443 ' to confirm closure.

Evidence: Before restricting access, capture the full running ACL and interface configuration via 'get system interface' and 'show firewall policy' — the exploit targets the HTTPS management interface via a crafted websocket request to the Node.js management daemon (CVE-2024-55591 abuses jsconsole websocket handler), so document current exposure of TCP 443/8443 on all management IPs. Export FortiOS system event logs (Log & Report > System Events) for the 30-day window preceding containment to preserve pre-restriction admin session records, API access logs, and any super-admin account creation events that occurred while the interface was exposed.

Step 2: Detection — Query firewall and VPN logs for anomalous websocket connections to the FortiOS management interface, unexpected super-admin account creation or privilege changes, and repeated failed authentication attempts against Fortinet VPN endpoints (T1110 brute-force pattern). Review AU-2 event logging output for admin session initiations lacking corresponding MFA events. Check for new or unrecognized administrator accounts (CIS 5.1 — account inventory). Hunt for outbound connections to unknown IPs that may indicate custom C2 activity (T1041). Cross-reference any identified IPs and hashes against CISA KEV and threat feeds.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use FortiOS built-in CLI queries: 'execute log filter category event' then 'execute log filter field action login' to extract admin login events; pipe output to a text file for manual review. For super-admin creation, query 'diagnose debug cloudinit show' and review 'config system admin' — any account not in your baseline is suspect. For websocket anomalies, enable packet capture on the management interface via 'diagnose sniffer packet "port 443" 6 0 l' and pipe through Wireshark filtering on websocket upgrade requests ('http.upgrade == "websocket"'). Cross-reference outbound IPs against the CISA KEV feed (downloadable as JSON from cisa.gov/known-exploited-vulnerabilities-catalog) using a simple Python or PowerShell script to flag matches.

Evidence: Capture FortiOS admin event logs (Log & Report > System Events, subtype 'admin') focusing on event type 'login' with source IPs outside your admin CIDR — CVE-2024-55591 exploitation produces an authenticated admin session with no valid credential exchange recorded, appearing as a session with 'type=event subtype=system action=login' entries lacking a preceding successful MFA event. Preserve FortiAuthenticator or SSL-VPN authentication logs for T1110 brute-force indicators (repeated 'Login Failed' events from single or rotating IPs). Extract the full admin account table ('config system admin / show') and diff it against your change management records to identify accounts created during the exploitation window — Gentlemen group actors have been documented creating backdoor super-admin accounts post-exploitation.

Step 3: Eradication — Apply FortiGuard-issued patches per FG-IR-24-535 to upgrade FortiOS to a fixed version above 7.0.16 and FortiProxy to a fixed version above 7.0.19 / 7.2.12. Rotate all administrative credentials on affected devices immediately following patching (D3-CRO — Credential Rotation). Audit all administrator accounts created or modified during the exposure window and remove unauthorized accounts (D3-LAM — Local Account Monitoring, NIST AC-2 — Account Management, CIS 5.3 — Disable Dormant Accounts). Review and revoke any API tokens or VPN credentials that may have been compromised.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 5.3 (Disable Dormant Accounts), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Download FortiOS firmware directly from support.fortinet.com (verify SHA256 checksum against Fortinet's published hash before flashing). Before patching, run 'config system admin / show full-configuration' and export to a secure out-of-band file — this is your pre-patch account baseline for diff comparison post-eradication. To enumerate and revoke API tokens, run 'config system api-user / show' from CLI and delete any unrecognized entries with 'delete '. For SSL-VPN credential revocation without a PAM tool, use FortiOS 'config user local' to force a password reset on all local VPN accounts and 'execute vpn sslvpn del-tunnel all' to terminate active sessions immediately.

Evidence: Before applying the patch, image or snapshot the FortiOS configuration ('execute backup config tftp ') to preserve the compromised state for forensic analysis — this captures any backdoor accounts, modified admin profiles, or altered SSL-VPN policies inserted by Gentlemen actors. Collect FortiOS configuration change logs (Log & Report > System Events, action='cfg-change') to establish a timeline of unauthorized modifications made via the auth bypass. Preserve any downloaded FortiProxy or FortiOS diagnostic logs ('diagnose debug report') which may contain artifacts of the jsconsole websocket exploitation session before the patch overwrites affected components.

Step 4: Recovery — After patching, validate that management interfaces are no longer accessible from untrusted networks. Confirm MFA is enforced on all administrative and VPN access paths (D3-MFA — Multi-factor Authentication, CIS 6.3 — Require MFA for Externally-Exposed Applications, CIS 6.4 — Require MFA for Remote Network Access, CIS 6.5 — Require MFA for Administrative Access). Re-baseline expected network behavior and monitor for residual C2 beaconing or lateral movement. Audit audit log integrity to confirm no tampering occurred during the intrusion window (NIST AU-9 — Protection of Audit Information).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate management interface closure post-patch using an external nmap scan ('nmap -p 443,8443,80 --open ') from outside your perimeter — any open result indicates ACL misconfiguration. For MFA enforcement verification on FortiOS without a commercial PAM, run 'show system admin' and confirm 'two-factor' is set to a non-'disable' value for every admin account; for SSL-VPN users, verify 'config user group' settings require two-factor auth group membership. For residual C2 detection without EDR, deploy Zeek (formerly Bro) or run Wireshark captures on egress segments filtering for periodic beaconing patterns (regular interval connections to single external IPs) using display filter 'ip.dst != && tcp.flags.syn == 1' and look for jitter-free 60/300-second interval connections characteristic of Gentlemen group C2 tooling.

Evidence: Compare FortiOS audit logs (Log & Report > System Events) from post-patch period against pre-incident baseline to identify log gaps or deletions that would indicate Gentlemen actors attempted log tampering (MITRE T1070.002 — Indicator Removal: Clear Linux or Mac System Logs). Capture current NetFlow or FortiGate traffic logs from the SSL-VPN concentrator and internal segments to establish a clean post-recovery baseline — any persistence mechanism (T1078 — Valid Accounts) installed by actors during the auth bypass window would appear as authenticated VPN or admin sessions from unusual source IPs or at unusual times relative to this new baseline. Verify

FortiOS syslog forwarding configuration ('config log syslogd setting') to confirm logs were forwarded to an external destination throughout the incident window and cross-check received log volume against on-device log counts to detect deletion.

Step 5: Post-Incident — Conduct a lessons-learned review covering: management interface exposure policies (NIST AC-17), patch cadence gaps against CISA KEV obligations (CIS 7.3 — Automated OS Patch Management), and VPN authentication strength (CIS 6.4). Evaluate whether AI-assisted phishing lures (T1566) reached internal users and assess security awareness training coverage. Document control gaps and update the vulnerability management process (CIS 7.1 — Establish and Maintain a Vulnerability Management Process). Consider adding FortiGate management interface traffic to continuous monitoring scope (NIST SI-4, AU-6 — Audit Record Review, Analysis, and Reporting).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST AC-17 (Remote Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For AI-assisted phishing (T1566) assessment without an email security gateway, export mail server message trace logs (Exchange: 'Get-MessageTrackingLog -EventId RECEIVE -Start -End ' or equivalent) and grep for domains/URLs registered within 30 days of the campaign start — a hallmark of AI-generated lure infrastructure. Use the free MxToolbox Header Analyzer against sampled inbound messages from the incident window to flag SPF/DKIM failures indicating spoofed sender domains. For ongoing FortiGate management interface monitoring without SIEM, write a cron job that runs 'grep "action=login" /var/log/fortios_event.log | awk -F"srcip=" "{print $2}"' hourly and alerts on any source IP outside your admin ACL. Document CVE-2024-55591 in your vulnerability register with CISA KEV citation and establish a 14-day SLA for KEV-listed vulnerabilities on internet-exposed network edge devices.

Evidence: Retrieve and preserve the complete FortiOS event log archive covering the full exposure window (from first vulnerable firmware version deployment through patch application) to support root cause analysis and any regulatory breach notification timeline reconstruction — Fortinet stores logs in '/var/log/' and remotely via configured syslog; confirm log completeness by correlating log record counts against known event frequency baselines. For AI-assisted phishing evaluation, collect and hash all suspicious email samples received during the campaign window and submit to VirusTotal or run through a local ClamAV scan with updated signatures to identify AI-generated lure documents; also review DNS query logs from internal resolvers for lookups to newly registered domains (WHOIS age under 30 days) that correlate with T1566 phishing delivery timeframes attributed to Gentlemen group activity.

Detection Guidance

Focus detection on three areas: management interface abuse, account manipulation, and C2 activity.

1. Management interface websocket anomalies: Review FortiOS event logs for unauthenticated or anomalous websocket sessions to the admin interface. Look for admin login events lacking a preceding credential prompt or MFA event. FortiOS logs these under the 'admin' event category; filter for source IPs outside expected management ranges.

2. Privilege escalation and account creation: Query for new super-admin account creation events or privilege modifications within the FortiOS admin audit log. Cross-reference against your CIS 5.1 account inventory. Any account not in the approved inventory is a high-priority indicator.

3. Brute-force against VPN: Correlate failed authentication events on Fortinet VPN endpoints. A spike in T1110-pattern failures followed by a successful login from the same or geographically distant IP is a strong indicator of compromise.

4. C2 beaconing: Monitor egress traffic from FortiGate appliances for periodic, low-volume connections to unfamiliar external IPs, consistent with custom C2 tooling (T1041). Behavioral baselines from your SIEM or NDR are the best reference point here.

5. AI-assisted phishing follow-on: If initial access is confirmed, hunt for T1566 delivery artifacts, emails with unusually well-crafted lures targeting employees. Check email gateway logs for messages referencing Fortinet, VPN access, or IT security themes delivered near the intrusion window.

D3FEND defensive techniques to prioritize for detection: D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis for configuration changes), D3-UAP (User Account Permissions review).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-55591`	Public proof-of-concept exploit for CVE-2024-55591 published by watchtowrlabs — confirms weaponized code is publicly accessible	HIGH

Framework Mappings

MITRE-ATTACK

- **T1110** — Brute Force
- **T1588.002** — Tool
- **T1486** — Data Encrypted for Impact
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1566** — Phishing

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110	Brute Force	Credential-Access

Technique ID	Technique Name	Tactic
T1588.002	Tool	Resource-Development
T1486	Data Encrypted for Impact	Impact
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
gemini	https://gbhackers.com/gentlemen-ransomware-exploits-fortinet-flaws-...	T3
CVE-2024-55591 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2024-55591	T1
CVE-2024-55591 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2024-55591	T3
Authentication bypass in Node.js websocket module - FortiGuard Labs	https://www.fortiguard.com/psirt/FG-IR-24-535	T3
watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-55591 - GitHub	https://github.com/watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-5...	T3

Generated 2026-06-03 19:09 UTC by TJS Security Command Center