INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-03 06:49 UTC

FortiBleed Access Brokers Escalate to Ransomware Deployment via Inc and Lynx Gangs, Exploit Nextcloud Zero-Day

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0616
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Fortinet FortiGate firewalls (FortiBleed-affected devices); Nextcloud (zero-day, version unspecified)
Published	2026-07-02T15:11:33
Discovery Source	Rss

Executive Summary

Threat actors who previously sold access to compromised Fortinet FortiGate firewalls have escalated operations, reportedly partnering with Inc and Lynx ransomware groups to deploy ransomware across victim environments. According to a single Dark Reading report from July 2, 2026, the campaign has also expanded to exploit an unspecified Nextcloud zero-day, though this claim has not been independently corroborated in the available source set. Organizations running FortiGate devices affected by the FortiBleed vulnerability and those using Nextcloud face elevated risk of ransomware deployment, data exfiltration, and extended operational disruption.

Technical Analysis

This campaign represents a kill-chain escalation from initial access brokerage to active ransomware deployment. The underlying access vector is the FortiBleed vulnerability in Fortinet FortiGate firewalls, associated with CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), and CWE-20 (Improper Input Validation). Prior reporting, corroborated by Arctic Wolf, documented malicious configuration changes on FortiGate devices via SSO accounts. The escalation phase, reported by Dark Reading (2026-07-02), describes partnerships with Inc and Lynx ransomware-as-a-service operations. A separate CyberScoop article references CVE-2026-24858, a FortiCloud SSO authentication bypass zero-day, though direct linkage to this specific campaign is unconfirmed in the source material. The reported Nextcloud zero-day component, version unspecified, is sourced exclusively from the single Dark Reading article; no independent

corroboration exists in the provided sources. MITRE ATT&CK techniques mapped to this campaign include T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1078 (Valid Accounts), T1005 (Data from Local System), T1083 (File and Directory Discovery), T1650 (Acquire Access), T1588.006 (Vulnerabilities), T1071 (Application Layer Protocol), T1570 (Lateral Tool Transfer), and T1486 (Data Encrypted for Impact). No specific IOCs have been published in the available source set. Patch status for the Nextcloud zero-day is unspecified; Fortinet remediation guidance should be sourced from official Fortinet advisories.

Action Checklist

1. Step 1: Containment. Immediately audit all FortiGate devices for unauthorized SSO account changes and unexpected configuration modifications, as documented by Arctic Wolf. Isolate any FortiGate devices that cannot be confirmed as uncompromised. As a precautionary measure pending vendor advisory, restrict internet-facing Nextcloud instances at the perimeter or apply compensating controls (WAF, IP allowlisting) until the reported zero-day is independently confirmed and patched.
2. Step 2: Detection. Review FortiGate management audit logs for unauthorized SSO account additions or configuration changes (reference Arctic Wolf blog for specific indicators). Search for anomalous authentication events mapped to NIST AU-6 (Audit Record Review, Analysis, and Reporting). Monitor for T1486 indicators: mass file encryption events, volume shadow copy deletion, and ransomware-associated process execution. Alert on lateral tool transfer activity (T1570) and unusual outbound application-layer traffic (T1071) from FortiGate management interfaces and Nextcloud servers.
3. Step 3: Eradication. Apply all available Fortinet security advisories addressing FortiBleed. If CVE-2026-24858 (FortiCloud SSO authentication bypass) is confirmed applicable to your deployment, apply patches per Fortinet guidance. Rotate all credentials, including SSO accounts, administrative accounts, and API keys, on affected FortiGate devices (D3-CRO: Credential Rotation). Remove any unauthorized accounts identified during audit (NIST AC-2: Account Management; CIS 5.3: Disable Dormant Accounts). Until a Nextcloud patch is available, apply compensating controls per vendor guidance.
4. Step 4: Recovery. Validate FortiGate configurations against known-good baselines following remediation (D3-SFA: System File Analysis; NIST CM controls). Confirm no persistence mechanisms remain on compromised devices. Restore Nextcloud services only after vendor confirmation or compensating controls are in place. Enforce MFA on all administrative and remote access paths (NIST AC-17: Remote Access; CIS 6.3: Require MFA for Externally-Exposed Applications; D3-MFA: Multi-factor Authentication).
5. Step 5: Post-Incident. Review whether FortiGate devices were properly inventoried and monitored per CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) and CIS 8.2 (Collect Audit Logs). Assess whether least-privilege principles (NIST AC-6) were enforced on firewall management accounts. Evaluate third-party access and external system policies (NIST AC-20). Document gaps and update incident response playbooks to account for access-broker-to-ransomware escalation patterns.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and external IR retainer immediately upon confirmation that Inc or Lynx ransomware payloads have executed in the environment, or upon discovery of data exfiltration evidence from Nextcloud (which may trigger breach notification obligations under GDPR, HIPAA, or applicable state law depending on data classification), or if the internal team lacks the forensic capability to acquire and analyze memory from potentially compromised FortiGate devices running FortiOS.
Recovery Notes	Following containment and eradication, restore FortiGate devices only from verified clean firmware images obtained directly from Fortinet's support portal with hash-verified downloads, not from potentially compromised management backups. Monitor FortiGate event logs and downstream authentication infrastructure (Active Directory, RADIUS) for re-emergence of unauthorized SSO accounts or configuration changes for a minimum of 30 days post-recovery, given that access brokers may retain sold credentials and re-attempt access after initial remediation. Nextcloud services should remain restricted at the perimeter until Fortinet and the Nextcloud project issue formal advisories with patch availability, and any restoration should be preceded by a file integrity check of the Nextcloud application directory against known-good hashes.
Forensic Artifacts	FortiGate system event logs (Log & Report > System Events) filtered on admin account creation, SSO account modification, and configuration change events — these directly evidence the unauthorized account additions Arctic Wolf documented as FortiBleed-phase access-broker activity | FortiGate running configuration export ('show full-configuration' captured via CLI) diffed against pre-incident backup — unauthorized 'config system sso-admin' or 'config system admin' blocks with unrecognized usernames indicate access-broker persistence | Windows Volume Shadow Copy service event logs (Event ID 7036 in System log, Event ID 524 in Security log) and VSS snapshot inventory ('vssadmin list shadows') from domain-joined hosts — deletion of shadow copies is a consistent pre-encryption step for both Inc and Lynx ransomware operators | Nextcloud application log (/var/www/nextcloud/data/nextcloud.log) and web server access log filtered for anomalous WebDAV methods (PROPFIND, MKCOL, PUT) and HTTP 5xx responses from previously unreachable endpoints — these would be the primary indicators of zero-day exploitation attempts against the unpatched Nextcloud instance | Memory image (WinPmem/LiME output) from any host exhibiting ransomware indicators, preserving in-memory Inc or Lynx encryptor artifacts, C2 beacon threads, and injected code prior to process termination or system isolation

Per-Action IR Details

Step 1: Containment — Immediately audit all FortiGate devices for unauthorized SSO account changes and unexpected configuration modifications, as documented by Arctic Wolf. Isolate any FortiGate devices that cannot be confirmed as uncompromised. Restrict internet-facing Nextcloud instances at the perimeter until a vendor advisory is available for the reported zero-day.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-4 (Information Flow Enforcement), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'get system admin' and 'get system sso-admin' via FortiGate CLI on each device to enumerate admin and SSO accounts; diff output against your last known-good admin export. Block Nextcloud HTTPS (TCP/443 and TCP/80) at the upstream border router or ISP edge using an ACL rather than relying on FortiGate itself, which may be the compromised chokepoint. A 2-person team can complete CLI audits across up to 10 devices in under 2 hours with a prepared checklist.

Evidence: Before isolating any FortiGate device, capture: (1) full running configuration ('show full-configuration' output), (2) current admin and SSO account list ('get system admin', 'get system sso-admin'), (3) active session table ('get system session list'), (4) FortiGate event log export covering the prior 90 days (Log & Report > System Events, filter on 'admin' and 'sso' object types), and (5) netstat equivalent via 'diagnose sys tcp-summary' to record active management-plane connections. For Nextcloud, export the Apache/nginx access log and Nextcloud application log (/var/www/nextcloud/data/nextcloud.log) prior to any perimeter block, preserving timestamps of any anomalous POST or PROPFIND requests.

Step 2: Detection — Review FortiGate management audit logs for unauthorized SSO account additions or configuration changes (reference Arctic Wolf blog for specific indicators). Search for anomalous authentication events mapped to NIST AU-6 (Audit Record Review, Analysis, and Reporting). Monitor for T1486 indicators: mass file encryption events, volume shadow copy deletion, and ransomware-associated process execution. Alert on lateral tool transfer activity (T1570) and unusual outbound application-layer traffic (T1071) from FortiGate management interfaces and Nextcloud servers.

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 AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use FortiGate's built-in Log & Report console filtered on event type 'config-change' and 'admin-login' for the past 90 days; export to CSV and grep for accounts not in your authorized admin list. On Windows endpoints, deploy Sysmon (config targeting Event IDs 1, 11, 23) and parse with 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 1 -and $_.Message -match "vssadmin|wmic shadowcopy"}' to catch VSS deletion. Use a Sigma rule mapped to Sysmon EID 1 for processes (e.g., vssadmin.exe delete shadows, wbadmin delete catalog) spawned from unusual parent processes consistent with Inc or Lynx ransomware deployment chains.

Evidence: Before any active response that would alter log state, collect and hash (SHA-256) the following volatile artifacts: (1) FortiGate event logs filtered on 'sso', 'admin', and 'config' object changes — export raw syslog if forwarding is configured; (2) Windows Security Event Log Event ID 4720 (account creation), 4728/4732 (group membership changes), and 4625/4624 (logon failures and successes) on domain controllers for any accounts traceable to FortiGate SSO integration; (3) memory image (via WinPmem or LiME) from any host exhibiting mass file rename activity, capturing in-memory ransomware payloads before process termination; (4) Nextcloud application log entries showing abnormal WebDAV PROPFIND, PUT, or MKCOL requests that would indicate zero-day exploitation reconnaissance or staging.

Step 3: Eradication — Apply all available Fortinet security advisories addressing FortiBleed and, if confirmed applicable, CVE-2026-24858 (FortiCloud SSO authentication bypass). Rotate all credentials — including SSO accounts, administrative accounts, and API keys — on affected FortiGate devices (D3-CRO: Credential Rotation). Remove any unauthorized accounts identified during audit (NIST AC-2: Account Management; CIS 5.3: Disable Dormant Accounts). Until a Nextcloud patch is available, apply compensating controls per vendor guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), 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: If automated patch management is unavailable, manually download FortiOS firmware from support.fortinet.com (verify SHA-256 against Fortinet's published hash before flashing), apply via FortiGate GUI under System > Firmware. Credential rotation for API keys: enumerate via 'config system api-user' in FortiGate CLI, delete all existing API users, and recreate with least-privilege profiles. For Nextcloud without a patch, disable the affected endpoint or module in config/config.php and restrict access to trusted IP ranges via Nextcloud's trusted_domains and allow_local_remote_servers settings.

Evidence: Before applying any patch or rotating credentials — both of which alter live authentication state — capture: (1) a final snapshot of all current FortiGate admin, SSO, and API user configurations ('show system admin', 'show system sso-admin', 'show system api-user') as forensic baseline of attacker-created accounts; (2) FortiGate session table dump ('diagnose sys session list') to document any active sessions that may represent access-broker persistence; (3) on any host potentially staged for ransomware deployment, acquire a RAM image and run 'netstat -ano' and 'Get-ScheduledTask' to capture in-memory payloads and scheduled task persistence (common Inc/Lynx pre-deployment mechanisms) before credential rotation breaks their C2 channel and they may trigger payload execution.

Step 4: Recovery — Validate FortiGate configurations against known-good baselines following remediation (D3-SFA: System File Analysis; NIST CM controls). Confirm no persistence mechanisms remain on compromised devices. Restore Nextcloud services only after vendor confirmation or compensating controls are in place. Enforce MFA on all administrative and remote access paths (NIST AC-17: Remote Access; CIS 6.3: Require MFA for Externally-Exposed Applications; D3-MFA: Multi-factor Authentication).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), 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 FortiGate configuration integrity by exporting the running config post-remediation ('execute backup config ftp ') and running a line-by-line diff against your pre-incident backup using 'diff -u baseline.conf current.conf', flagging any 'set sso' or 'config system admin' blocks that differ. For MFA enforcement without an enterprise IdP, enable FortiToken (hardware or mobile) for all FortiGate admin accounts via System > Administrators > Edit > Two-factor Authentication. For Nextcloud, enable TOTP via the built-in Two-Factor TOTP Provider app prior to restoring public access.

Evidence: Before restoring any service to production, verify that no attacker-established scheduled tasks, cron jobs, or startup scripts persist: on FortiGate, run 'show system automation-stitch' and 'show system automation-trigger' to identify any attacker-configured automation; on Nextcloud hosts, run 'crontab -l -u www-data' and inspect /etc/cron.d/ for entries added during the compromise window. Document the post-remediation configuration export with SHA-256 hash as the new forensic baseline, stored offline and immutably (write-once media or locked S3 bucket) to support future integrity comparisons.

Step 5: Post-Incident — Review whether FortiGate devices were properly inventoried and monitored per CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) and CIS 8.2 (Collect Audit Logs). Assess whether least-privilege principles (NIST AC-6) were enforced on firewall management accounts. Evaluate third-party access and external system policies (NIST AC-20). Document gaps and update incident response playbooks to account for access-broker-to-ransomware escalation patterns.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), NIST AU-11 (Audit Record Retention), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Conduct a tabletop exercise specifically simulating the access-broker-to-ransomware escalation pattern seen with Inc and Lynx groups: begin with the assumption that a FortiGate SSO account has been silently sold, and walk through detection timelines, isolation decisions, and communications. Use osquery ('SELECT * FROM users; SELECT * FROM logged_in_users;') scheduled as a weekly cron to continuously validate the authorized account baseline on all network appliances accessible via SSH. Document the exercise findings and delta from this incident in a structured after-action report shared with leadership within 2 weeks of full recovery.

Evidence: Preserve the complete forensic record for a minimum of 12 months given the ransomware group involvement (Inc and Lynx are known to exfiltrate before encrypting, creating potential breach notification obligations): retain FortiGate event log exports, memory images, network capture files (pcap), and all recovered malicious artifacts under chain-of-custody documentation. Archive the Arctic Wolf indicators used during this response alongside the

internal timeline to enable future threat-hunting queries and to benchmark detection latency for playbook improvement.

Detection Guidance

Primary detection focus is on FortiGate management plane activity and ransomware staging behavior. Review FortiGate audit logs for unauthorized SSO account creation or modification; Arctic Wolf's blog documents the specific configuration change pattern. Correlate authentication events against NIST AU-3 (Content of Audit Records) requirements: who authenticated, from where, at what time, and what changes followed. For ransomware staging, hunt for T1486 indicators: rapid file modification across network shares, Volume Shadow Copy deletion commands, and known ransomware process hashes if threat intelligence feeds publish them. Monitor for T1570 (Lateral Tool Transfer): unexpected file drops or execution from management interfaces. For Nextcloud, log all API and authentication events and alert on anomalous access patterns pending vendor advisory. Apply D3-LAM (Local Account Monitoring) on both FortiGate management accounts and Nextcloud administrator accounts. No specific IOCs (IPs, domains, hashes) are available in the current source set; monitor threat intelligence feeds for Inc and Lynx IOC updates.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1005** — Data from Local System
- **T1083** — File and Directory Discovery
- **T1650** — Acquire Access
- **T1588.006** — Vulnerabilities
- **T1190** — Exploit Public-Facing Application
- **T1071** — Application Layer Protocol
- **T1570** — Lateral Tool Transfer
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation

- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **IR-4** — Incident Handling
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **16.10** — Apply Secure Design Principles in Application Architectures

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1005	Data from Local System	Collection
T1083	File and Directory Discovery	Discovery
T1650	Acquire Access	Resource-Development
T1588.006	Vulnerabilities	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1071	Application Layer Protocol	Command-And-Control
T1570	Lateral Tool Transfer	Lateral-Movement
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/fortibleed-actors-i...	T2
Arctic Wolf Observes Malicious Configuration Changes On Fortinet ...	https://arcticwolf.com/resources/blog/arctic-wolf-observes-maliciou...	T3
Is Fortinet That Bad? - Networking & Firewalls	https://forums.lawrencesystems.com/t/is-fortinet-that-bad/23830	T3
Fortinet's latest zero-day vulnerability carries frustrating familiarities ...	https://cyberscoop.com/ortinet-zero-day-cve-2026-24858-forticloud-s...	T2

Generated 2026-07-03 06:49 UTC by TJS Security Command Center