INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-09 15:01 UTC

ntopng through 6.6 is vulnerable to Predictable Session Identifier which can lead to Session Hijacking. HTTP session identifiers in src/HTTPserver.cpp use weak time-seeded pseudo-randomness during session creation. As a result, fresh authenticated logins can receive deterministic or colliding session cookies under attacker-controlled timing.

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0401
Type	CVE Vulnerability
CVE ID	CVE-2026-38968
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0038 (30th percentile)
Affected Products	ntopng through 6.6; Microsoft Azure Linux 3.0 package azl3 ntopng 5.2.1-6
Published	2026-07-09T01:50:30
Discovery Source	Msrc Patch Tuesday

Executive Summary

A critical vulnerability in ntopng, a widely used network traffic monitoring platform, allows attackers to predict or forge session cookies for freshly authenticated users, enabling account takeover without stealing credentials. Affected versions include ntopng through 6.6 and the Microsoft Azure Linux 3.0 package azl3 ntopng 5.2.1-6, disclosed as part of Microsoft's July 2026 Patch Tuesday with a CVSS score of 9.8 (Critical). Organizations running ntopng in network operations or security monitoring roles face risk of unauthorized access to network visibility tooling, which could allow an attacker to observe traffic, suppress alerts, or pivot to connected infrastructure.

Technical Analysis

CVE-2026-38968 is a predictable session identifier vulnerability (CWE-330: Use of Insufficiently Random Values; CWE-384: Session Fixation) in ntopng through version 6.6. The root cause is in src/HTTPserver.cpp, where HTTP session identifiers are generated using a weak time-seeded pseudo-random number generator (PRNG) at session creation time. Because the seed is time-based and predictable under attacker-controlled timing conditions, an adversary can enumerate or collide with session tokens issued to freshly authenticated users, enabling session hijacking (MITRE T1539) or valid account abuse (T1078) without requiring credential compromise. The attack requires no authentication and carries a CVSS 3.x base score of 9.8. The Microsoft-packaged version azl3 ntopng 5.2.1-6 on Azure Linux 3.0 is also confirmed affected per the MSRC advisory (July 2026 Patch Tuesday). No exploitation in the wild has been confirmed in available source material; this CVE is not currently listed in the CISA Known Exploited Vulnerabilities Catalog (KEV status: false). EPSS score is 0.00379 (29.98th percentile) as of available data. No patch version has been specified in the source material, operators should monitor the ntopng upstream repository and the MSRC advisory for remediation guidance.

Action Checklist

1. Step 1: Containment, Immediately restrict network access to the ntopng web interface (default port 3000) to trusted internal IP ranges or VPN-only access. If ntopng is internet-facing, take the web interface offline or block external access at the firewall until a patched version is confirmed available. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Audit ntopng web server access logs for unusual session activity: repeated session ID enumeration attempts, rapid successive logins from the same source IP, or authenticated sessions originating from unexpected IP addresses. Correlate against NIST AU-6 (Audit Record Review, Analysis, and Reporting). Query for access patterns targeting the ntopng HTTP interface (default port 3000) in your network flow and proxy logs. No specific IOC patterns (IP, domain, hash) are confirmed in the available source material.
3. Step 3: Eradication, Apply the vendor-issued patch or updated package when available. For Azure Linux 3.0 deployments, monitor the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-38968 for an updated azl3 ntopng package superseding 5.2.1-6. For upstream ntopng, monitor the ntopng GitHub repository for a release addressing CVE-2026-38968. As an interim measure, enforce session timeout settings to the shortest operationally acceptable interval to reduce the window for session collision attacks. Reference: NIST AC-12 (Session Termination), NIST IA-4 (Identifier Management).
4. Step 4: Recovery, After patching, invalidate all active ntopng sessions and require re-authentication. Verify the updated version is running by confirming the binary version string and package version. Monitor ntopng access logs for at least 72 hours post-remediation for anomalous session activity. Re-enable external or broader network access only after patch confirmation. Reference: NIST AU-6, CIS 8.2 (Collect Audit Logs).
5. Step 5: Post-Incident, Review all network monitoring tools in the environment for similar PRNG-based session management weaknesses. Assess whether ntopng had visibility into sensitive network segments; if so, treat any session active during the exposure window as potentially compromised and review associated access. Implement controls requiring MFA for all ntopng administrative access. Reference: NIST AC-6 (Least Privilege), CIS 6.5 (Require MFA for Administrative Access), NIST IA-2(1) (Multi-factor Authentication).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal/compliance if ntopng had visibility into network segments processing PII, PHI, PCI-DSS cardholder data, or OT/ICS traffic during the exposure window, as any authenticated session active during that period must be treated as potentially compromised and may trigger breach notification obligations.
Recovery Notes	After applying the vendor patch for CVE-2026-38968, verify the fixed ntopng binary is running via `ntopng --version` and confirm the package version matches the patched release in the MSRC advisory or ntopng GitHub changelog before re-enabling any external access to port 3000. Monitor ntopng HTTP access logs continuously for at least 72 hours post-remediation, specifically watching for session cookie values that exhibit sequential or near-sequential patterns (indicating residual PRNG predictability or an attacker replaying a pre-patch captured cookie). Retain all pre-patch logs, memory artifacts, and session records for a minimum of 90 days under the incident case to support any downstream forensic review or regulatory inquiry.
Forensic Artifacts	ntopng HTTP access log (`/var/log/ntopng/ntopng.log` or path defined in `/etc/ntopng/ntopng.conf`): contains session cookie values, source IPs, timestamps, and HTTP response codes — primary artifact for identifying session enumeration attempts, cookie collisions, or authenticated sessions from unexpected sources during the CVE-2026-38968 exposure window | In-memory ntopng process dump (`gcore $(pgrep ntopng)`): preserves the live session table and PRNG state from the vulnerable src/HTTPserver.cpp session initialization code — must be captured before any service restart, patch application, or host isolation that clears memory | Network packet capture of TCP port 3000 traffic (via `tcpdump -i any port 3000 -w ntopng_traffic.pcap`): enables extraction and analysis of HTTP session cookie values across multiple connections to detect sequential or time-correlated tokens consistent with the weak time-seeded PRNG vulnerability mechanism | ntopng user database and session records (Redis data under `/var/lib/ntopng//` or ntopng's SQLite database): documents which accounts held authenticated sessions during the exposure window and provides the session IDs issued by the vulnerable PRNG for timeline reconstruction | ntopng-captured flow and traffic data for the exposure window (stored in ntopng's RRD files or ClickHouse/MySQL backend per deployment configuration): since ntopng functions as a network monitor, an attacker with a hijacked session may have queried or exported sensitive flow data — these records establish what network intelligence was accessible to any compromised session

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to the ntopng web interface (default port 3000) to trusted internal IP ranges or VPN-only access. If ntopng is internet-facing, take the web interface offline or block external access at the firewall until a patched version is confirmed available. 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)

Compensating: On Linux hosts: `iptables -I INPUT -p tcp --dport 3000 ! -s -j DROP` to immediately restrict ntopng HTTP access to approved ranges. On Windows Server with ntopng deployed: use Windows Defender Firewall (`netsh advfirewall firewall add rule name='Block ntopng ext' dir=in action=block protocol=tcp localport=3000`). Verify the rule

is active with `iptables -L -n -v` or `netsh advfirewall firewall show rule name='Block ntopng ext'`. Document the rule with timestamp for the incident record.

Evidence: Before restricting firewall access, capture: (1) active TCP connections to port 3000 via `ss -tnp sport = :3000` or `netstat -anp | grep :3000` to document all current sessions and source IPs; (2) the ntopng process memory state if feasible (`gcore `) to preserve in-memory session table contents generated by the weak PRNG in src/HTTPserver.cpp; (3) current ntopng session cookie values from any open browser sessions on analyst workstations used to administer ntopng. These artifacts are destroyed once the service is restarted or connections are dropped.

Step 2: Detection — Audit ntopng web server access logs for unusual session activity: repeated session ID enumeration attempts, rapid successive logins from the same source IP, or authenticated sessions originating from unexpected IP addresses. Correlate against NIST AU-6 (Audit Record Review, Analysis, and Reporting). Query for access patterns targeting the ntopng HTTP interface (default port 3000) in your network flow and proxy logs. No specific IOC patterns (IP, domain, hash) are confirmed in the available source material.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Parse ntopng's HTTP access log (default path `/var/log/ntopng/ntopng.log` or the path set in `/etc/ntopng/ntopng.conf`) using: `awk '$9 == 200 {print $1, $7}' /var/log/ntopng/ntopng.log | sort | uniq -c | sort -rn` to surface source IPs with high authenticated request volume. Extract session cookie values from log entries and look for sequential or near-sequential values (indicating time-seeded PRNG collision) with: `grep 'Cookie:' /var/log/ntopng/ntopng.log | grep -oP 'session=\K[^;]+' | sort | uniq -c | sort -rn`. Capture network flows to/from port 3000 with `tcpdump -i any -w ntopng_capture.pcap port 3000` for offline Wireshark analysis of session token patterns across connections.

Evidence: Forensic evidence to collect before any session invalidation or service restart: (1) full ntopng HTTP access log snapshot (`cp /var/log/ntopng/ntopng.log /forensics/ntopng_access_$(date +%s).log`); (2) active session table dump if accessible via ntopng REST API (`curl -u admin: http://localhost:3000/lua/rest/v2/get/flow/active.lua`) to document which session tokens are currently authenticated; (3) system authentication log (`/var/log/auth.log` or `journalctl -u ntopng --since '48 hours ago'`) for OS-level login events correlated with ntopng session creation timestamps; (4) network capture of port 3000 traffic already in progress on any network tap or span port, preserved before containment action drops connections.

Step 3: Eradication — Apply the vendor-issued patch or updated package when available. For Azure Linux 3.0 deployments, monitor the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-38968 for an updated azl3 ntopng package superseding 5.2.1-6. For upstream ntopng, monitor the ntopng GitHub repository for a release addressing CVE-2026-38968. As an interim measure, enforce session timeout settings to the shortest operationally acceptable interval to reduce the window for session collision attacks. Reference: NIST AC-12 (Session Termination), D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-12 (Session Termination), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Before patching, verify the currently installed ntopng version with `ntopng --version` or `rpm -q ntopng` (Azure Linux 3.0) or `dpkg -l ntopng` (Debian-based). For Azure Linux 3.0, apply the updated azl3 package once published via `tdnf update ntopng` and verify with `rpm -q ntopng`. For upstream ntopng, build or install the fixed release per the ntopng GitHub release page and confirm `ntopng --version` reflects the patched build. As interim PRNG

mitigation, reduce session lifetime in `/etc/ntopng/ntopng.conf` by setting `--session-max-duration=` to the minimum operationally viable value (e.g., 900 seconds) and restart the service: `systemctl restart ntopng`.

Evidence: Before applying the patch or restarting ntopng (both of which destroy in-memory session state): (1) acquire a full memory dump of the ntopng process (`gcore $(pgrep ntopng) -o /forensics/ntopng_pre_patch.core`) to preserve the PRNG state and in-memory session map from src/HTTPserver.cpp; (2) record all currently authenticated session cookie values and associated source IPs from the active session log or REST API; (3) snapshot the ntopng binary pre-patch (`sha256sum $(which ntopng) > /forensics/ntopng_binary_pre_patch.sha256`) to document the vulnerable artifact for the post-incident record. These artifacts cannot be recovered after service restart or reimaging.

Step 4: Recovery — After patching, invalidate all active ntopng sessions and require re-authentication. Verify the updated version is running by confirming the binary version string and package version. Monitor ntopng access logs for at least 72 hours post-remediation for anomalous session activity. Re-enable external or broader network access only after patch confirmation. Reference: NIST AU-6, CIS 8.2 (Collect Audit Logs).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-12 (Session Termination), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Force invalidation of all active ntopng sessions by restarting the ntopng service post-patch (`systemctl restart ntopng`), which clears in-memory session state generated by the fixed src/HTTPserver.cpp. Confirm the patched version string with `ntopng --version` and record the output. For the 72-hour monitoring window, run a recurring log parse every 15 minutes: `watch -n 900 'awk \'$9==200{print $1,$7}\' /var/log/ntopng/ntopng.log | sort | uniq -c | sort -rn | head -20'` to catch anomalous session reuse. Re-enable port 3000 firewall access only after this command returns the patched version and no unexpected authenticated sessions appear.

Evidence: Before re-enabling broad network access and invalidating sessions: (1) preserve a final snapshot of the ntopng HTTP access log immediately post-patch as a clean-baseline reference (`cp /var/log/ntopng/ntopng.log /forensics/ntopng_post_patch_baseline_$(date +%s).log`); (2) document the new ntopng binary hash (`sha256sum $(which ntopng) >> /forensics/ntopng_binary_post_patch.sha256`) to confirm the patched artifact is running; (3) retain all pre-patch logs and memory artifacts under the incident case number per your log retention policy (NIST AU-11) for potential post-incident review of whether any session hijacking occurred during the exposure window.

Step 5: Post-Incident — Review all network monitoring tools in the environment for similar PRNG-based session management weaknesses. Assess whether ntopng had visibility into sensitive network segments; if so, treat any session active during the exposure window as potentially compromised and review associated access. Implement controls requiring MFA for all ntopng administrative access. Reference: NIST AC-6 (Least Privilege), CIS 6.5 (Require MFA for Administrative Access), D3-MFA (Multi-factor Authentication).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.5 (Require MFA for Administrative Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Enumerate all other network monitoring tools (e.g., Zabbix, Grafana, LibreNMS, Cacti) deployed in the environment and audit their session management implementation for time-seeded PRNG patterns — check vendor changelogs or open source code for `time()`, `rand()`, or `srand(time())` calls in session initialization paths. For ntopng MFA enforcement, if ntopng itself lacks native MFA support, place it behind an authenticating reverse proxy (e.g., nginx with oauth2-proxy and an OIDC provider) to enforce MFA at the network layer before requests reach port 3000. Document any accounts that were authenticated to ntopng during the CVE-2026-38968 exposure window and review ntopng's captured network traffic data for evidence of unauthorized queries against sensitive segments.

Evidence: For the post-incident review, compile: (1) the full list of ntopng user accounts active during the exposure window, extracted from ntopng's user database (`/var/lib/ntopng//` Redis data or ntopng's SQLite DB) and correlated against the pre-patch HTTP access logs; (2) ntopng's own captured flow data for the exposure window — since ntopng monitors network traffic, its stored pcap or flow records may show what an attacker with a hijacked session could have

viewed or exfiltrated from monitored segments; (3) a timeline of all authenticated sessions during the exposure period, mapped against the weak PRNG seed window (correlate login timestamps with `time()` values to assess whether session IDs were predictable), to support a determination of whether any session hijacking occurred.

Detection Guidance

Query web server and proxy logs for the ntopng HTTP interface (default TCP port 3000) for the following behavioral indicators: (1) High-frequency GET or POST requests to the ntopng login or session endpoints from a single source IP within a short time window, consistent with session ID enumeration. (2) Authenticated sessions (HTTP 200 responses to protected pages) immediately following a burst of failed or probing requests from the same source, suggesting successful session collision. (3) Authenticated activity from IP addresses that did not perform the originating login, check for session tokens appearing across multiple source IPs. Log sources: ntopng access logs, network flow data (NetFlow/IPFIX), WAF or reverse proxy logs if deployed in front of ntopng. Relevant NIST controls: AU-2 (Event Logging), AU-3 (Content of Audit Records), AU-6 (Audit Record Review). No confirmed IOCs (IPs, domains, hashes) are present in the available source material. Detection should be behavioral, not signature-based, until threat intelligence with specific IOCs is published.

Framework Mappings

MITRE-ATTACK

- **T1539** — Steal Web Session Cookie
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-38968	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Jul	T1
CVE-2026-38968 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-38968	T1
Known Exploited Vulnerabilities Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2026-38968	https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/...	T3

Generated 2026-07-09 15:01 UTC by TJS Security Command Center