INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 19:02 UTC

Commodity BadIIS MaaS Ecosystem Targets IIS Servers While Defenders Face Credential Exposure and Biometric Data Loss

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0349
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft IIS servers, NGINX (njs module), TP-Link devices, Adobe Photoshop, OpenVPN, Gen Digital Norton VPN, CISA GitHub infrastructure, NYC Health + Hospitals systems, OpenClaw
Published	2026-05-21T18:00:14+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

A commercially distributed malware toolkit is actively compromising Microsoft IIS web servers at scale, enabling traffic hijacking, SEO fraud, and persistent access sold as a service to multiple criminal operators. Simultaneously, CISA inadvertently published sensitive credentials to a public GitHub repository, and NYC Health + Hospitals confirmed a breach exposing biometric data for approximately 1.8 million patients. Collectively, these incidents signal elevated risk across federal web infrastructure, healthcare systems, and any organization running IIS servers without current hardening controls.

Technical Analysis

Cisco Talos documented the BadIIS malware-as-a-service ecosystem, attributed to Chinese-speaking cybercrime operators, enabling persistent IIS server compromise via IIS native-code modules (T1505.004, IIS Components). Attackers abuse valid accounts (T1078) and event-triggered execution (T1546) to maintain persistence, proxying traffic through compromised infrastructure (T1090.002) for SEO fraud and command-and-control (T1071.001). Relevant CWEs include CWE-284 (Improper Access Control) and CWE-269 (Improper Privilege Management). Separately, CISA exposed credentials in a public GitHub repository (CWE-256, Plaintext Credential Storage, CWE-312, Cleartext Storage of Sensitive Information; MITRE T1552.001, Credentials in Files). NYC Health + Hospitals suffered a breach resulting in irreversible biometric data loss, with regulatory implications under HIPAA given the healthcare context (CWE-284). Cisco

Talos also disclosed multiple vulnerabilities across TP-Link devices, Adobe Photoshop, OpenVPN, and Gen Digital Norton VPN, covering heap-based buffer overflow (CWE-122) and privilege escalation (CWE-269) classes. No CVE IDs were provided in the source data; no CISA KEV designation is recorded for this item. Primary attribution and technical detail trace to Cisco Talos research.

Action Checklist

1. Step 1: Containment. Audit all IIS servers for unauthorized native-code modules (IIS Components, T1505.004). Disable or remove any unrecognized ISAPI filters or modules immediately. Restrict IIS management interfaces to internal networks only (NIST AC-17, CIS 4.4). For TP-Link, OpenVPN, and Norton VPN deployments, isolate affected devices from internet-facing segments pending patch review.
2. Step 2: Detection. Query IIS logs for anomalous HTTP response patterns indicating traffic redirection or SEO injection (unusual Location headers, 301/302 chains to external domains). Review Windows Event Logs for new module registrations under IIS (Event IDs 4688, 7045). Audit GitHub repositories and CI/CD pipeline secrets for any exposed credentials following the CISA pattern; cross-reference against CIS 8.2 (Collect Audit Logs) and NIST AU-6 (Audit Record Review, Analysis, and Reporting). Search for IOC patterns from Talos reporting: anomalous IIS worker process child processes, unexpected outbound connections from IIS hosts on non-standard ports.
3. Step 3: Eradication. Remove all unauthorized IIS modules and restore server configurations from known-good baselines (NIST CM controls, CIS 4.6). Rotate all credentials confirmed or suspected to be exposed in public repositories immediately, following NIST IA controls and credential rotation procedures. Apply available vendor patches for TP-Link, Adobe Photoshop, OpenVPN, and Gen Digital Norton VPN from official vendor channels; track against CIS 7.3 and 7.4 (Automated OS and Application Patch Management). Revoke and reissue any API keys or service account tokens present in affected GitHub repositories.
4. Step 4: Recovery. Validate IIS server integrity by comparing installed modules against a verified software inventory (CIS 2.1) before restoring to production. Confirm outbound traffic from IIS hosts returns to expected baselines using SIEM correlation. Re-enable services only after successful credential rotation and module audit. Monitor IIS servers for 30 days post-remediation for reinfection indicators, consistent with NIST SI-4 (System Monitoring). For biometric data breach at NYC Health + Hospitals: affected individuals cannot reset biometric identifiers; notify affected parties and review substitute authentication mechanisms per NIST IA controls.
5. Step 5: Post-Incident. Implement pre-commit secret scanning on all repositories, including internal and public-facing GitHub organizations, directly addressing the CISA credential exposure pattern (NIST AU-9, Credential Hardening, CIS 5.2). Enforce MFA on all IIS management interfaces and administrative accounts (CIS 6.5). Establish a formal software inventory and module allowlist for IIS deployments (CIS 2.1, CIS 2.3). Conduct a lessons-learned review covering credential management, IIS hardening baselines, and third-party VPN and device patch cadence. If biometric data is processed, evaluate whether collection is necessary and document retention limits per CIS 3.4 and CIS 3.5.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel and senior leadership if any IIS server confirmed with BadIIS module serves regulated data (PHI, PII, PCI-scoped cardholder data), if any GitHub-exposed credential provides access to cloud infrastructure or production systems, or if biometric data breach at NYC Health + Hospitals triggers applicable state or federal breach notification deadlines — HIPAA requires notification to HHS within 60 days for breaches affecting 500 or more individuals in a state.
Recovery Notes	IIS servers should not be returned to production until the module allowlist comparison, applicationHost.config restore, and full credential rotation are independently verified — BadIIS operators have demonstrated the ability to re-implant via compromised administrative credentials, making partial remediation a reinfection risk. Monitor all recovered IIS hosts for 30 days using Sysmon Event ID 1 and 3 alerts scoped to w3wp.exe child process creation and non-standard outbound connections, reviewing alerts daily for the first two weeks given active campaign status. For the biometric breach component, maintain a separate recovery track for affected NYC Health + Hospitals individuals including fallback authentication enrollment tracking, as biometric identifiers cannot be reissued and the remediation timeline for affected individuals extends indefinitely.
Forensic Artifacts	IIS W3C access logs (%SystemDrive%\inetpub\logs\LogFiles\W3SVC*): Search for 301/302 responses where the Location header value is an external domain not owned by the organization — BadIIS injects these redirects at the ISAPI filter layer to hijack organic search traffic for SEO fraud without modifying application code. | IIS ApplicationHost.config (%windir%\system32\inetsrv\config\applicationHost.config): BadIIS persists by registering a native-code DLL as a globalModules or modules entry in this file; compare the file's last-modified timestamp and module list against your version-controlled baseline to identify unauthorized additions. | Windows System Event Log — Event ID 7045 (New Service or Module Installed): IIS module registration via appcmd or direct config manipulation may generate this event; filter for DLL paths outside expected IIS system directories (e.g., outside %windir%\system32\inetsrv\) as BadIIS modules are typically dropped to non-standard paths. | Sysmon Event ID 1 (Process Create) filtered on ParentImage containing w3wp.exe: BadIIS operator post-exploitation activity — lateral movement, credential dumping, or C2 beacon execution — will appear as child processes of the IIS worker process, a relationship that has no legitimate baseline in a properly hardened IIS deployment. | GitHub organization audit log (exported via GitHub API or Settings > Audit Log): Contains push event records with committer identity, timestamp, and repository name for any commit that introduced credentials to a public or internal repository — directly applicable to reconstructing the CISA-pattern exposure timeline and identifying whether additional secrets beyond those already identified were committed.

Per-Action IR Details

Step 1: Containment — Audit all IIS servers for unauthorized native-code modules (IIS Components, T1505.004). Disable or remove any unrecognized ISAPI filters or modules immediately. Restrict IIS management interfaces to internal networks only, enforcing NIST AC-17 (Remote Access) and CIS 4.4 (Implement and Manage a Firewall on Servers). For TP-Link, OpenVPN, and Norton VPN deployments, isolate affected devices from internet-facing segments pending patch review.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 2.3 (Address Unauthorized Software)

Compensating: Run 'appcmd list module /text:*' on each IIS host to enumerate all loaded modules and ISAPI filters; pipe output to a file and diff against a known-good baseline captured before incident. Use PowerShell

'Get-WebConfiguration system.webServer/modules' to extract module DLL paths and cross-check file hashes with Get-FileHash against an internal allowlist. Block IIS Management Service port 8172 and Remote Administration port 80/443 at the Windows Firewall using 'netsh advfirewall firewall add rule' for all source IPs outside the management VLAN. For TP-Link and VPN devices with no available patch, null-route their WAN interfaces or place them behind an ACL permitting only specific internal management IPs.

Evidence: Before disabling any module, capture the full IIS module list via 'appcmd list module' and preserve DLL file paths, hashes (SHA-256), and timestamps. Dump the IIS ApplicationHost.config file from %windir%\system32\inetsrv\config\applicationHost.config, which BadIIS uses to persist module registrations. Record IIS worker process (w3wp.exe) parent-child relationships from a live Process List with PID/PPID, command-line arguments, and loaded DLLs using Sysinternals Process Explorer or 'wmic process get name,processid,parentprocessid,commandline'. Capture current Windows Firewall rules and any outbound connections from IIS hosts using 'netstat -ano' correlated with PID-to-process mapping before isolation blocks C2 traffic.

Step 2: Detection — Query IIS logs for anomalous HTTP response patterns indicating traffic redirection or SEO injection (unusual Location headers, 301/302 chains to external domains). Review Windows Event Logs for new module registrations under IIS (Event IDs 4688, 7045). Audit GitHub repositories and CI/CD pipeline secrets for any exposed credentials following the CISA pattern; cross-reference against CIS 8.2 (Collect Audit Logs) and NIST AU-6 (Audit Record Review, Analysis, and Reporting). Search for IOC patterns from Talos reporting: anomalous IIS worker process child processes, unexpected outbound connections from IIS hosts on non-standard ports.

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 SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Parse IIS W3C access logs (default path: %SystemDrive%\inetpub\logs\LogFiles\W3SVC*) using PowerShell 'Select-String' or 'Import-Csv' filtering for sc-status values 301 or 302 where cs-uri-stem does not match your known application routes and cs-host points to external domains — BadIIS SEO injection characteristically inserts redirect chains toward affiliate or ad-fraud domains. Deploy Sysmon with configuration targeting w3wp.exe: log Event ID 1 (Process Create) for any child process spawned by w3wp.exe (cmd.exe, powershell.exe, certutil.exe) and Event ID 3 (Network Connection) for w3wp.exe outbound on ports other than 80/443/8080. For GitHub secret detection, run truffleHog (open source) or gitleaks against your repository history with 'gitleaks detect --source . --log-opts=--all' to surface any committed API keys, tokens, or passwords matching the CISA exposure pattern.

Evidence: Collect IIS W3C logs from all virtual hosts for the 90-day window preceding detection, preserving original timestamps and ensuring log rotation has not purged earlier entries — BadIIS may have been resident for weeks before SEO fraud activity surfaces in traffic analytics. Export Windows System Event Log filtering for Event ID 7045 (New Service Installed) and Security Event Log for Event ID 4688 (Process Creation) where NewProcessName contains w3wp.exe as ParentProcessName, covering the same 90-day window. Pull GitHub audit log exports (available under Organization Settings > Audit Log) for any push events to repositories containing infrastructure secrets, focusing on the timeframe bracketing the CISA-pattern exposure. Capture DNS query logs from the IIS host (if DNS client logging is enabled via 'auditpol /set /subcategory:"DNS query" /success:enable') to identify C2 or ad-fraud domain resolutions initiated by w3wp.exe.

Step 3: Eradication — Remove all unauthorized IIS modules and restore server configurations from known-good baselines per NIST CM controls and CIS 4.6 (Securely Manage Enterprise Assets and Software). Rotate all credentials confirmed or suspected to be exposed in public repositories immediately, following NIST IA controls and D3-CRO (Credential Rotation). Apply available vendor patches for TP-Link, Adobe Photoshop, OpenVPN, and Gen Digital Norton VPN from official vendor channels; track against CIS 7.3 and 7.4 (Automated OS and Application Patch Management). Revoke and reissue any API keys or service account tokens present in affected GitHub repositories.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-2 (Baseline Configuration), NIST CM-7 (Least Functionality), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Remove BadIIS-implanted modules by unregistering them with 'appcmd delete module /module.name:' and deleting the backing DLL after confirming its SHA-256 hash does not match any legitimate Microsoft or third-party module from your software inventory. Restore applicationHost.config from a version-controlled backup, then run IIS Reset ('iisreset /restart') and re-verify the module list matches the allowlist. For credential rotation without a PAM tool, use a structured spreadsheet tracking each exposed secret (GitHub token, service account password, API key), its rotation status, and the rotation timestamp — prioritize secrets with IIS management, Azure DevOps pipeline, or cloud provider access first, as those represent the highest blast radius from the CISA-pattern exposure. Apply TP-Link, OpenVPN, and Norton VPN patches by downloading binaries directly from vendor support portals with SHA-256 hash verification before installation.

Evidence: Before removing any module DLL, image it forensically using a tool such as FTK Imager or 'dd' equivalent on Windows (via Sysinternals or EDD) for later malware analysis — BadIIS modules are native-code IIS components that may contain unique C2 configuration, victim tracking identifiers, or affiliate operator tags embedded in the binary. Preserve the pre-restoration applicationHost.config with its modification timestamp as evidence of unauthorized module registration. Document all rotated credentials with before/after rotation timestamps for audit trail under NIST AU-10 (Non-Repudiation). Capture GitHub audit log entries confirming revocation of exposed tokens before and after rotation.

Step 4: Recovery — Validate IIS server integrity by comparing installed modules against a verified software inventory (CIS 2.1) before restoring to production. Confirm outbound traffic from IIS hosts returns to expected baselines using SIEM correlation. Re-enable services only after successful credential rotation and module audit. Monitor IIS servers for 30 days post-remediation for reinfection indicators, consistent with NIST SI-4 (System Monitoring). For biometric data breach at NYC Health + Hospitals: affected individuals cannot reset biometric identifiers; notify affected parties and review substitute authentication mechanisms per NIST IA controls.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST IA-3 (Device Identification and Authentication), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Before returning each IIS server to production, run 'appcmd list module /text:*' and compare output against your pre-incident allowlist using a PowerShell diff script — flag any module whose DLL path, file hash, or registration timestamp does not match the baseline. Deploy Sysmon Event ID 3 (Network Connection) monitoring on all IIS hosts for 30 days post-restoration, alerting on any w3wp.exe outbound connection to a destination not in an approved IP/FQDN allowlist, which would indicate BadIIS reinfection or a secondary implant surviving eradication. For the NYC Health + Hospitals biometric breach, document the specific biometric modalities exposed (fingerprint, facial, iris) in the breach notification and work with clinical operations to implement PIN or token-based fallback authentication for affected individuals, referencing NIST IA-5 enhancement (1) for authenticator management in healthcare contexts. Note: escalation for this breach to HHS Office for Civil Rights under HIPAA Breach Notification Rule is required given the 1.8 million affected individuals.

Evidence: Capture a post-remediation snapshot of the IIS module list, applicationHost.config, and w3wp.exe process tree within 1 hour of service restoration as a new verified baseline. Retain 30 days of Sysmon and IIS W3C logs post-restoration in write-protected storage to support reinfection detection and any regulatory forensic requests related to the biometric data breach. Document the integrity validation results (module hash comparisons, config diffs) as evidence of due diligence for both the BadIIS remediation and any future regulatory inquiry into the NYC Health + Hospitals breach.

Step 5: Post-Incident — Implement pre-commit secret scanning on all repositories, including internal and public-facing GitHub organizations, directly addressing the CISA credential exposure pattern (NIST AU-9, D3-CH — Credential Hardening, CIS 5.2). Enforce MFA on all IIS management interfaces and administrative accounts (CIS 6.5, D3-MFA). Establish a formal software inventory and module allowlist for IIS deployments (CIS 2.1, CIS 2.3). Conduct a lessons-learned review covering credential management, IIS hardening baselines, and third-party VPN and device patch cadence. If biometric data is processed, evaluate whether collection is necessary and document retention limits per CIS 3.4 and CIS 3.5.

NIST Phase: Post Incident

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

Controls: NIST AU-9 (Protection of Audit Information), NIST CM-7 (Least Functionality), NIST IA-2 (Identification and Authentication — Organizational Users), NIST RA-3 (Risk Assessment), CIS 5.2 (Use Unique Passwords), CIS 6.5 (Require MFA for Administrative Access), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data)

Compensating: Implement gitleaks or truffleHog as a pre-commit Git hook ('gitleaks protect --staged') on all developer workstations and as a CI/CD pipeline step in GitHub Actions or Jenkins — this directly closes the CISA-pattern exposure where credentials were committed to a public repository without automated detection. Enforce MFA on IIS management by requiring Windows Hello for Business or a TOTP-based authenticator (e.g., Google Authenticator with a RADIUS bridge) for all Remote Desktop and IIS Manager sessions, and document this requirement in your IIS hardening baseline. Build the IIS module allowlist as a plain-text file of approved DLL names and SHA-256 hashes under version control, and schedule a monthly PowerShell job to run 'appcmd list module' on all IIS hosts and alert on any deviation — this addresses the T1505.004 persistence mechanism that made BadIIS effective at scale. For biometric data minimization, conduct a data flow mapping exercise to identify all systems ingesting biometric identifiers and apply CIS 3.5 disposal procedures to any data retained beyond the documented operational need.

Evidence: Produce a lessons-learned report documenting the timeline from BadIIS initial access (estimated from earliest anomalous IIS log entries) to detection, containment, and eradication, quantifying dwell time — this is required input for updating detection rule tuning and IIS module monitoring thresholds. Archive the full forensic package (pre-remediation module snapshots, applicationHost.config versions, Sysmon logs, IIS W3C logs, GitHub audit exports) with retention consistent with NIST AU-11 (Audit Record Retention) and any applicable breach notification regulatory requirements for the biometric data exposure. Document all post-incident control improvements with owner, implementation date, and validation method to support the next risk assessment cycle under NIST RA-3 (Risk Assessment).

Detection Guidance

IIS compromise indicators: Check %SystemRoot%\System32\inetsrv\config\applicationHost.config for unrecognized globalModules or handlers. Monitor IIS worker process (w3wp.exe) for unexpected child process spawning via Windows Event ID 4688. Alert on outbound HTTP/HTTPS connections from IIS hosts to uncommon external destinations, particularly those not in your CDN or application dependency list. SEO injection pattern: look for HTTP responses containing injected meta tags, hidden links, or Location headers redirecting to gambling, pharmaceutical, or unrelated commercial domains. Credential exposure: scan all GitHub repositories (public and private) using tools such as truffleHog or gitleaks for secrets, API keys, and plaintext passwords; cross-reference recent commit history. NIST AU-2 and AU-12 require logging authentication events, privilege use, and configuration changes; confirm these are active on all IIS hosts. For TP-Link, OpenVPN, and Norton VPN: review vendor security advisories for specific indicators; monitor device logs for privilege escalation attempts (CWE-269) and unexpected process crashes consistent with heap overflow exploitation (CWE-122). NIST SI-7 (System File Integrity Monitoring) and NIST AU-2 (Audit Events) apply directly: alert on modifications to IIS configuration files and on local account creation or privilege changes on IIS hosts.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://blog.talosintelligence.com/the-art-of-being-ungovernable/`	Cisco Talos primary BadIIS MaaS campaign analysis — refer for full IOC list published by Talos	HIGH
URL	`https://blog.talosintelligence.com/welcome-to-the-party-pal-2/`	Cisco Talos supplemental campaign reporting on BadIIS ecosystem	HIGH
URL	`https://blog.talosintelligence.com/tp-link-photoshop-openvpn-norton-vpn-vulnerabilities/`	Cisco Talos vulnerability disclosure for TP-Link, Adobe Photoshop, OpenVPN, Gen Digital Norton VPN	HIGH

Framework Mappings

MITRE-ATTACK

- **T1090.002** — External Proxy
- **T1071.001** — Web Protocols
- **T1078** — Valid Accounts
- **T1546** — Event Triggered Execution
- **T1555.003** — Credentials from Web Browsers
- **T1552.001** — Credentials In Files
- **T1190** — Exploit Public-Facing Application
- **T1608.004** — Drive-by Target
- **T1584** — Compromise Infrastructure
- **T1588.001** — Malware
- **T1505.004** — IIS Components
- **T1491.002** — External Defacement
- **T1068** — Exploitation for Privilege Escalation
- **T1565.002** — Transmitted Data Manipulation

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection

- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090.002	External Proxy	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1546	Event Triggered Execution	Privilege-Escalation
T1555.003	Credentials from Web Browsers	Credential-Access
T1552.001	Credentials In Files	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1608.004	Drive-by Target	Resource-Development
T1584	Compromise Infrastructure	Resource-Development
T1588.001	Malware	Resource-Development
T1505.004	IIS Components	Persistence
T1491.002	External Defacement	Impact
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1565.002	Transmitted Data Manipulation	Impact

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/the-art-of-being-ungovernable/	T3
	https://blog.talosintelligence.com/welcome-to-the-party-pal-2/	T3
TP-Link, Photoshop, OpenVPN, Norton VPN vulnerabilities	https://blog.talosintelligence.com/tp-link-photoshop-openvpn-norton...	T3
Talos recently disclosed eight vulnerabilities in TP-Link, and one ...	https://x.com/TalosSecurity/status/2056763518234304682	T3
TP-Link, Photoshop, OpenVPN, Norton VPN vulnerabilities - Reddit	https://www.reddit.com/r/SecOpsDaily/comments/1thrhrm/tplink_photos...	T3

Generated 2026-05-21 19:02 UTC by TJS Security Command Center