INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-07 18:35 UTC

GRU's Forest Blizzard Turns Home Routers Into Spy Infrastructure: DNS Hijacking Enables Mass OAuth Token Theft from Microsoft 365

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0155
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	SOHO/home routers (multiple unspecified vendors), Microsoft Outlook on the web, Microsoft 365, Microsoft Entra ID
Published	2026-04-07T13:02:44
Discovery Source	Rss

Executive Summary

Russia's GRU-affiliated group Forest Blizzard (APT28) compromised over 18,000 home and small-office routers beginning August 2025, peaking in December 2025, to intercept Microsoft 365 authentication traffic and steal OAuth session tokens without touching endpoint devices (Microsoft Security Blog, 2026-04-07). More than 200 organizations across government, energy, telecommunications, and IT sectors were affected. The attack bypasses MFA protections tied to password theft alone; stolen OAuth tokens grant persistent, authenticated access to Microsoft 365 and Entra ID environments until explicitly revoked.

Technical Analysis

Forest Blizzard (MITRE ATT&CK Group G0007, identified by Microsoft as GRU-affiliated APT28) conducted an adversary-in-the-middle (AiTM) campaign by first gaining access to SOHO and home routers via weak or default credentials and unpatched firmware (no single CVE assigned). The actor reconfigured DNS settings on compromised routers to redirect victim traffic destined for Microsoft Outlook on the web (OWA) to attacker-controlled infrastructure. TLS interception (AiTM) was then applied to decrypt OAuth 2.0 authentication flows in transit, harvesting session tokens and credentials for Microsoft 365 and Microsoft Entra ID without deploying malware on victim endpoints. Relevant CWEs: CWE-300 (Channel Accessible by Non-Endpoint), CWE-295 (Improper Certificate Validation), CWE-923 (Improper Restriction of Communication Channel to Intended Endpoints), CWE-290 (Authentication Bypass by Spoofing). MITRE ATT&CK techniques include T1557 (Adversary-in-the-Middle), T1557.002 (ARP/DNS Poisoning), T1040 (Network Sniffing), T1539 (Steal

Web Session Cookie), T1556 (Modify Authentication Process), T1584.008 (Compromise Infrastructure: Network Devices), T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1071.001 and T1071.004 (Application Layer Protocol). No patch for a specific CVE exists; the router compromise vector relied on operator misconfigurations and unpatched firmware. Source: Microsoft Security Blog, 2026-04-07.

Action Checklist

1. Step 1: Containment. Immediately audit all SOHO and home routers used by remote workers, branch offices, and any network perimeter devices for unauthorized DNS server changes. Compare current DNS settings against known-good baselines. Temporarily restrict or require VPN with split-tunnel controls for any remote worker whose router DNS configuration cannot be verified. Prioritize devices running firmware versions more than 6 months old or from vendors with delayed firmware release cycles.
2. Step 2: Detection. Query Microsoft Entra ID (Azure AD) sign-in logs for OAuth token issuances associated with unexpected IP geolocation, unfamiliar device registration, or sign-in timestamps inconsistent with user activity patterns. Review Entra ID audit logs for token grants where AuthenticationDetails does not contain MFA method confirmation. Search Microsoft 365 Unified Audit Log for anomalous mailbox access, mail forwarding rules, or OAuth app consent grants post-August 2025. Check DNS query logs on routers and DNS resolvers for unexpected upstream resolvers not matching your provisioned servers. Alert on Entra ID Conditional Access policy failures from known IP ranges paired with successful token issuance from different IPs.
3. Step 3: Eradication. Reset all SOHO and home router administrative credentials to unique, strong passwords. Update router firmware to the latest vendor-released version immediately. Restore DNS settings to authoritative, organization-provisioned servers (or known-good ISP defaults for home workers). For any confirmed or suspected token compromise, revoke all active OAuth refresh tokens for affected accounts via Microsoft Entra ID using Microsoft Graph PowerShell (Revoke-MgUserSignInSession) or Azure AD module legacy cmdlet (Revoke-AzureADSignedInUserAllRefreshTokens). Require re-authentication with fresh MFA for affected users. Review and revoke any OAuth app consent grants created during the August-December 2025 window that cannot be verified as user-initiated.
4. Step 4: Recovery. Validate that DNS settings on all audited routers now point to correct, authorized resolvers and have not reverted. Confirm no unauthorized mail forwarding rules, inbox rules, or OAuth delegations remain on affected Microsoft 365 accounts. Monitor Entra ID sign-in logs and Conditional Access reports for a minimum of 30 days post-remediation for anomalous token usage. Re-enroll affected users in MFA if token revocation was performed. Verify that Entra ID Conditional Access policies enforce token binding or Continuous Access Evaluation (CAE) where supported.
5. Step 5: Post-Incident. This campaign exploited the absence of phishing-resistant MFA (FIDO2/hardware keys) and lack of token binding enforcement. Accelerate deployment of phishing-resistant MFA per CISA guidance (https://www.cisa.gov/sites/default/files/2023-03/csso-scuba-guidance_document-hybrid_identity_solutions_architecture-2023.03.22-final.pdf, human validation recommended). Evaluate Entra ID Conditional Access policies to enforce compliant device requirements and CAE. Establish a router firmware and credential audit process for all network devices in scope, including remote worker equipment. Map control gaps to NIST SP 800-53 SC-8 (Transmission Confidentiality and Integrity), IA-3 (Device Identification and Authentication), and SI-3 (Malicious Code Protection) for GRC tracking.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and breach notification counsel immediately if Entra ID audit logs confirm OAuth token issuance to IPs geolocating outside the organization's known user geography between August 2025 and present, or if any affected accounts hold access to regulated data (PII, PHI, CUI, financial records), as this constitutes unauthorized access triggering breach notification obligations under GDPR, HIPAA, or applicable state privacy laws.
Recovery Notes	Recovery is not complete until every affected user account has been re-enrolled in MFA following token revocation AND a clean DNS state has been re-verified on all remote worker routers — performing one without the other leaves either the interception path or the stolen credential available to Forest Blizzard. Monitor Entra ID Conditional Access and Sign-in Risk reports daily for a minimum of 30 days post-remediation, specifically watching for legacy authentication protocol sign-ins (IMAP, POP3, SMTP AUTH) which bypass CAE and token binding protections and represent the most likely Forest Blizzard fallback persistence vector. If any user account shows sign-in activity from the same anomalous IP ranges identified during investigation after token revocation, treat as active recompromise and re-enter containment phase immediately.
Forensic Artifacts	Microsoft Entra ID Sign-in Logs (retention: 30 days free / 90 days P1/P2): query for OAuth token grants to 'login.microsoftonline.com' where 'token_claims_codes' field lacks 'mfa' claim AND source IP does not match known corporate or VPN egress ranges — these entries represent tokens Forest Blizzard harvested by intercepting the OAuth authorization code flow via the rogue DNS resolver | Microsoft 365 Unified Audit Log — Operations 'Add delegated permission grant' and 'Consent to application' with timestamps between August 1 2025 and December 31 2025: these entries record OAuth app consent grants that Forest Blizzard may have silently registered using stolen tokens to create persistent delegated access to victim mailboxes without requiring ongoing DNS interception | Router administration interface syslog or configuration export: the malicious DNS server IP addresses configured on WAN/LAN interfaces are the primary network-layer evidence of Forest Blizzard compromise — preserve these before any reset as they can be cross-referenced against known GRU command-and-control infrastructure reported by Microsoft MSTIC and NSA/CISA advisories on APT28 operational infrastructure | DNS resolver query logs from the rogue upstream server period: any DNS response for 'login.microsoftonline.com' or 'outlook.office365.com' that returned a non-Microsoft IP (outside Microsoft's published IP ranges in the O365 IP/URL web service) is direct evidence of the adversary-in-the-middle DNS hijack — these logs, if preserved from the router or ISP, establish exactly which users' authentication traffic was intercepted and the duration of exposure | Microsoft 365 mailbox inbox rule export (via 'Get-InboxRule' PowerShell): Forest Blizzard's post-compromise objective using stolen OAuth tokens was intelligence collection — inbox rules forwarding email to external addresses or marking messages as read are the persistence artifacts left after token use, and their creation timestamps map directly to when specific tokens were successfully exploited against each victim account

Per-Action IR Details

Step 1: Containment — Immediately audit all SOHO and home routers used by remote workers, branch offices, and any network perimeter devices for unauthorized DNS server changes. Compare current DNS settings against known-good baselines. Temporarily restrict or require VPN with split-tunnel controls for any remote worker whose router DNS configuration cannot be verified. Prioritize devices from vendors without recent firmware releases.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected network segments and prevent further token interception by Forest Blizzard's rogue DNS infrastructure before additional OAuth flows are hijacked

Controls: NIST IR-4 (Incident Handling), NIST SC-8 (Transmission Confidentiality and Integrity), NIST IA-3 (Device Identification and Authentication), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For a 2-person team without enterprise NAC: run a PowerShell script across VPN-connected endpoints — 'Get-DnsClientServerAddress' — to pull current DNS resolver IPs and diff against your baseline list; flag any resolver not matching your authoritative servers (e.g., 8.8.8.8, 1.1.1.1, or your internal resolver). For routers you cannot query programmatically, distribute a self-attestation form to remote workers with step-by-step instructions to check router DNS settings (browser to 192.168.1.1, screenshot DNS fields). Block outbound UDP/TCP 53 at your VPN gateway firewall for all remote worker traffic except to your designated resolvers — this prevents Forest Blizzard's rogue resolvers from answering Microsoft 365 authentication queries even if the router remains misconfigured.

Evidence: BEFORE changing any router settings: capture current DNS server IP addresses configured on the WAN and LAN interfaces (screenshot or export from router admin UI at 192.168.x.1); capture router syslog or admin access logs showing when DNS settings were last changed (typically under Administration > System Log or equivalent); export DHCP lease tables to identify which devices received the rogue resolver address; if router supports it, export DNS query logs showing upstream resolver queries to GRU-controlled IPs; preserve a full router configuration backup file before any reset, as it contains the malicious DNS entries as timestamped evidence of the intrusion window.

Step 2: Detection — Query Microsoft Entra ID (Azure AD) sign-in logs for OAuth token issuances associated with unexpected IP geolocation, unfamiliar device registration, or sign-in timestamps inconsistent with user activity patterns. Review Entra ID audit logs for token grants without corresponding MFA claims (token_claims_codes lacking 'mfa'). Search Microsoft 365 Unified Audit Log for anomalous mailbox access, mail forwarding rules, or OAuth app consent grants post-August 2025. Check DNS query logs on routers and DNS resolvers for unexpected upstream resolvers not matching your provisioned servers. Alert on Entra ID Conditional Access policy failures from known IP ranges paired with successful token issuance from different IPs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate Entra ID token issuance anomalies with DNS hijack indicators to confirm Forest Blizzard interception of Microsoft 365 OAuth flows and establish the scope of affected accounts

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Microsoft's free tooling directly: in Entra ID portal, run Sign-in Logs with filter 'App = Microsoft Office' AND 'Status = Success' AND date range August 1 2025 to present — export to CSV and sort by 'IP address' column to identify sign-ins from non-employee geographies (Russia, Eastern Europe, or residential ISP ranges inconsistent with your user base). Use PowerShell with the Microsoft Graph module: 'Get-MgAuditLogSignIn -Filter "appDisplayName eq \'Microsoft Office\'" | Where-Object { $_.conditionalAccessStatus -eq \'notApplied\' }' to find token grants that bypassed Conditional Access. For DNS detection without SIEM, use osquery on managed endpoints: 'SELECT * FROM dns_resolvers;' to enumerate configured resolvers, and cross-reference against your baseline. Deploy the free Sigma rule 'azure_ad_oauth_phishing.yml' (available on SigmaHQ GitHub) mapped to Entra ID log schema to detect token grants from impossible-travel IP pairs.

Evidence: Before querying logs, preserve immutable exports: download Entra ID Sign-in Logs for all users covering August 1 2025 to present (maximum 30-day retention in free tier — export immediately to avoid log expiration); export the Microsoft 365 Unified Audit Log via PowerShell 'Search-UnifiedAuditLog -StartDate 08/01/2025 -EndDate [today] -RecordType AzureActiveDirectoryAccountLogon' to capture OAuth consent grant events (Operation: 'Add delegated permission grant', 'Consent to application'); pull Entra ID Audit Logs for all 'Update user' and 'Add member to role' events in the same window; capture router DNS query logs (syslog export) showing resolution requests for 'login.microsoftonline.com' and 'outlook.office365.com' that returned non-Microsoft IP addresses — this is the direct evidence of Forest Blizzard's DNS interception of the OAuth authorization endpoint.

Step 3: Eradication — Reset all SOHO and home router administrative credentials to unique, strong passwords. Update router firmware to the latest vendor-released version immediately. Restore DNS settings to authoritative, organization-provisioned servers (or known-good ISP defaults for home workers). For any confirmed or suspected token compromise, revoke all active OAuth refresh tokens for affected accounts via Microsoft Entra ID (PowerShell: Revoke-AzureADUserAllRefreshToken or via Entra admin portal). Require re-authentication with fresh MFA for affected users. Review and revoke any OAuth app consent grants created during the August–December 2025 window that cannot be verified as user-initiated.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove Forest Blizzard's persistent access vectors by invalidating all OAuth refresh tokens harvested via DNS interception and eliminating the rogue DNS configuration that enabled the interception

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-3 (Device Identification and Authentication), NIST AC-2 (Account Management) — for OAuth app consent revocation, CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For token revocation without Entra P2 licensing: use the free Azure AD PowerShell command 'Revoke-AzureADUserAllRefreshToken -ObjectId [UserObjectID]' for each affected account — batch this with 'Get-AzureADUser | ForEach-Object { Revoke-AzureADUserAllRefreshToken -ObjectId $_.ObjectId }' for bulk revocation across all potentially affected users. For OAuth consent grant audit without a CASB tool, run 'Get-MgOAuth2PermissionGrant | Where-Object { $_.ConsentType -eq "Principal" }' via Microsoft Graph PowerShell and pipe output to CSV — manually review any grants created between August 1 and December 31 2025 against your known authorized app list. For router firmware updates on unmanaged home devices, provide workers a vendor-specific one-page instruction sheet; require photographic evidence of firmware version post-update as attestation. Use free router security scanner 'RouterSploit' (read-only audit mode) to verify the router no longer exposes default credentials or unpatched CVEs post-remediation.

Evidence: Before executing token revocations: export the full list of active OAuth refresh token sessions for all affected accounts via 'Get-MgUserAuthenticationMethod' and 'Get-MgUserSignInActivity' — this establishes which sessions were live at time of revocation and provides the scope for breach notification analysis; document all OAuth app consent grants present in the tenant with their creation timestamps before revocation, as grants created during the August–December 2025 window without user initiation are direct forensic evidence of Forest Blizzard persistence; capture router admin interface screenshots showing the malicious DNS server IPs before restoration — these constitute evidence of the infrastructure compromise and support threat intelligence sharing with CISA/MS-ISAC.

Step 4: Recovery — Validate that DNS settings on all audited routers now point to correct, authorized resolvers and have not reverted. Confirm no unauthorized mail forwarding rules, inbox rules, or OAuth delegations remain on affected Microsoft 365 accounts. Monitor Entra ID sign-in logs and Conditional Access reports for a minimum of 30 days post-remediation for anomalous token usage. Re-enroll affected users in MFA if token revocation was performed. Verify that Entra ID Conditional Access policies enforce token binding or Continuous Access Evaluation (CAE) where supported.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore verified-clean Microsoft 365 authentication posture and confirm Forest Blizzard's OAuth persistence mechanisms have been fully removed before resuming normal operations

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SC-8 (Transmission Confidentiality and Integrity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Without Entra ID P2 or a SIEM for 30-day monitoring: schedule a daily 15-minute manual review of Entra ID Sign-in Logs filtered to 'Risk level = medium or high' and 'IP address not in [your known corporate/VPN range]' — assign one team member per day on rotation. For mailbox rule auditing without E5 Defender, use PowerShell: 'Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object { $_.ForwardTo -ne $null -or $_.RedirectTo -ne $null }' to enumerate any forwarding rules that persist post-remediation. To verify DNS reversion hasn't occurred on

remote worker routers, send a weekly automated email asking users to confirm DNS settings via a simple self-check script (batch file or shell script that runs 'nslookup login.microsoftonline.com' and captures the resolver IP to a text file for submission). Enable Entra ID CAE via the free tier by navigating to Entra ID > Security > Continuous Access Evaluation and enabling for all users — this is a no-cost control that limits stolen OAuth token lifetime to near-real-time revocation.

Evidence: Before declaring recovery complete: run a final export of all Microsoft 365 inbox rules across affected accounts ('Get-Mailbox | Get-InboxRule | Export-CSV') and diff against the pre-incident baseline to confirm no Forest Blizzard-planted forwarding rules survive; pull a fresh Entra ID Conditional Access policy report to verify CAE and compliant device policies are enforced and not bypassed for any named locations or legacy authentication clients; document the DNS configuration state of all audited routers with timestamps as the post-remediation baseline — this establishes the clean-state reference for future drift detection and supports any regulatory breach notification documentation.

Step 5: Post-Incident — This campaign exploited the absence of phishing-resistant MFA (FIDO2/hardware keys) and lack of token binding enforcement. Accelerate deployment of phishing-resistant MFA per CISA guidance (https://www.cisa.gov/sites/default/files/2023-03/csso-scuba-guidance_document-hybrid_identity_solutions_architecture-2023.03.22-final.pdf — human validation recommended). Evaluate Entra ID Conditional Access policies to enforce compliant device requirements and CAE. Establish a router firmware and credential audit process for all network devices in scope, including remote worker equipment. Map control gaps to NIST SP 800-53 SC-8 (Transmission Confidentiality and Integrity), IA-3 (Device Identification and Authentication), and SI-3 (Malicious Code Protection) for GRC tracking.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review documenting how Forest Blizzard's DNS hijack defeated existing MFA controls and OAuth session protections, and use findings to drive FIDO2 deployment and network device governance improvements

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SC-8 (Transmission Confidentiality and Integrity), NIST IA-3 (Device Identification and Authentication), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without budget for FIDO2 hardware keys immediately: enable Microsoft Authenticator's 'Passwordless Phone Sign-in' (free with any Microsoft 365 license) as an interim phishing-resistant upgrade — this uses asymmetric cryptography and is significantly more resistant to OAuth interception than TOTP. For the router audit process without an MDM or NAC solution, create a quarterly self-attestation workflow using a free Microsoft Forms survey requiring remote workers to submit their router make, model, firmware version, and a screenshot of DNS settings — flag non-responders for IT follow-up. To detect future DNS hijacking without commercial DNS monitoring tools, deploy Pi-hole (free, open source) as a local DNS resolver for any office or branch environment and configure logging to a syslog server — forward logs to a free Elastic Stack instance for retention and alerting on resolver IP changes. Document all control gaps identified during this incident in a risk register entry referencing Forest Blizzard (APT28) as the threat actor and OAuth token theft via DNS hijack as the threat scenario for accurate risk scoring.

Evidence: For the post-incident lessons-learned record: compile the complete timeline of the incident from first malicious DNS change detected to final token revocation, using timestamps from router syslog exports, Entra ID sign-in log exports, and Unified Audit Log entries — this timeline is required for regulatory breach notification filings and for sharing with CISA's MS-ISAC if your organization qualifies; preserve all forensic exports (router configs, Entra ID logs, OAuth consent grant lists) for a minimum of 3 years per NIST AU-11 (Audit Record Retention) requirements; document the MITRE ATT&CK technique mapping for this campaign — T1557 (Adversary-in-the-Middle), T1071.001 (Application Layer Protocol: Web Protocols for OAuth flow interception), T1539 (Steal Web Session Cookie/Token), and T1098.003 (Account Manipulation: Additional Cloud Credentials) — for threat intelligence sharing and future detection rule development.

Detection Guidance

Primary detection surfaces are Microsoft Entra ID sign-in logs, the Microsoft 365 Unified Audit Log, and router/DNS infrastructure logs. Key behavioral indicators: (1) OAuth token grants from IP addresses inconsistent with user location or device history, especially where the issuing IP does not match the user's known network; (2) Entra ID sign-in events with AuthenticationDetails missing MFA method combined with downstream mailbox or SharePoint access; (3) newly registered OAuth application consents or mail forwarding rules created between August and December 2025 that users did not initiate; (4) DNS resolution on edge or SOHO routers pointing to IPs outside provisioned resolver ranges. In Microsoft Sentinel, query SigninLogs where ResultType == 0 and AuthenticationDetails does not contain MFA method cross-referenced with IPAddress outside known corporate egress. Alert on AuditLogs showing Set-MailboxRule or Add-MailboxPermission operations from service principals not in your approved list. Microsoft has not disclosed specific IOC IP ranges or domains at this publication date. Monitor MSTIC threat intelligence feeds and Microsoft Defender Threat Intelligence for Forest Blizzard IOC updates as they are released.

Indicators of Compromise

Type	Value	Context	Confidence
TTPS	`DNS reconfiguration on SOHO routers to attacker-controlled resolvers`	Forest Blizzard initial access technique — check router DNS settings against known-good baselines	HIGH
TTPS	`OAuth 2.0 token issuance without MFA claim in Entra ID sign-in logs`	Indicator of AiTM token interception — review token_claims in SigninLogs for missing MFA assertions	HIGH
TTPS	`Unauthorized mail forwarding rules or inbox rules created post-August 2025`	Post-compromise persistence mechanism — audit Unified Audit Log for Set-MailboxRule events from unexpected principals	HIGH
TTPS	`OAuth app consent grants created during August–December 2025 campaign window`	Possible persistence via delegated access — review Entra ID enterprise app consent logs for that period	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1556** — Modify Authentication Process
- **T1557** — Adversary-in-the-Middle
- **T1040** — Network Sniffing
- **T1071.004** — DNS
- **T1539** — Steal Web Session Cookie
- **T1584.008** — Network Devices

- **T1071.001** — Web Protocols
- **T1583.001** — Domains
- **T1190** — Exploit Public-Facing Application
- **T1557.002** — ARP Cache Poisoning
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **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
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1556	Modify Authentication Process	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1040	Network Sniffing	Credential-Access
T1071.004	DNS	Command-And-Control
T1539	Steal Web Session Cookie	Credential-Access
T1584.008	Network Devices	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1583.001	Domains	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1557.002	ARP Cache Poisoning	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.microsoft.com/en-us/security/blog/2026/04/07/soho-route...	T1
	https://krebsonsecurity.com/2026/04/russia-hacked-routers-to-steal-...	T3
	https://krebsonsecurity.com/2025/04/funding-expires-for-key-cyber-v...	T3
	https://krebsonsecurity.com/2026/04/germany-doxes-unkn-head-of-ru-r...	T3
Phishing actors exploit complex routing and misconfigurations to ...	https://www.microsoft.com/en-us/security/blog/2026/01/06/phishing-a...	T1

Generated 2026-04-07 18:35 UTC by TJS Security Command Center