INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 18:50 UTC

Silk Typhoon (Hafnium) Threat Actor Attribution Advances via U.S. Indictment and Extradition of MSS-Linked Operator

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0012
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft Exchange Server (2019 and earlier versions vulnerable during 2020-2021 campaign window)
Published	2026-04-28T03:57:00
Discovery Source	Rss

Executive Summary

U.S. authorities have extradited a Chinese national linked to the Silk Typhoon (Hafnium) espionage group, formally connecting the group to China's Shanghai State Security Bureau and a commercial front company. The campaign targeted COVID-19 research institutions and exploited Microsoft Exchange Server zero-days between 2020 and 2021. Organizations that ran unpatched Exchange servers during that window should treat this as a confirmation of the threat actor's capabilities and revisit historical logs for signs of compromise.

Technical Analysis

The indictment attributes the 2020-2021 Silk Typhoon (Hafnium) Exchange exploitation campaign to MSS operator Xu Zewei and the Shanghai State Security Bureau (SSSD), operating through front company Powerock Network. The campaign exploited Microsoft Exchange Server zero-days consistent with the ProxyLogon and ProxyShell vulnerability chains, covering CWE-287 (improper authentication), CWE-502 (deserialization of untrusted data), and CWE-78 (OS command injection). Affected versions: Exchange Server 2010 through 2019 (versions unpatched as of March-April 2021 for ProxyLogon; August 2021 for ProxyShell). MITRE ATT&CK techniques observed include T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter), T1560 (Archive Collected Data), T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1071 (Application Layer Protocol), T1591/T1589 (Gather Victim Information), T1583.001 (Acquire Infrastructure: Domains), and T1588.006 (Obtain Capabilities: Vulnerabilities). No new

CVEs or patches are associated with this indictment; the legal action advances attribution, not new technical disclosure. Exchange Server 2019 remains actively patched; the August 2025 update (KB5063221, latest as of that date) and December 2025 security updates are the current baselines per Microsoft and CISA.

Action Checklist

1. Step 1: Containment, If Exchange Server 2019 or earlier is internet-facing, confirm the latest Exchange security updates are applied (per current Microsoft Tech Community Exchange security advisories). At minimum, ensure December 2025 patches are in place. Verify no web shells remain in IIS virtual directories (OWA, ECP, Autodiscover paths) associated with ProxyLogon/ProxyShell exploitation.
2. Step 2: Detection, Search Exchange IIS logs (W3SVC1 and W3SVC2) from February 2020 through June 2021 for anomalous POST requests to /owa/auth/Current/, /ecp/DDI/, and /autodiscover/autodiscover.json. Correlate with CISA's Microsoft Exchange Server Security Best Practices advisory for known Hafnium IOC patterns. Use MITRE T1505.003 (web shell) and T1190 (exploitation) as hunting anchors in SIEM.
3. Step 3: Eradication, Apply all current Exchange Server security updates per Microsoft's cumulative update cadence. Remove any unauthorized ASPX files from Exchange virtual directories. Rotate credentials for any service accounts with Exchange access; Silk Typhoon used T1078 (Valid Accounts) for persistence after initial access.
4. Step 4: Recovery, Validate Exchange server integrity against Microsoft's recommended baseline (CISA Exchange Best Practices advisory). Monitor Exchange Application and Security event logs for recurrence of anomalous authentication (Event IDs 4625, 4648, 4672). Confirm no unauthorized forwarding rules or mailbox delegation persists (T1213 indicator).
5. Step 5: Post-Incident, This indictment confirms MSS-linked actors use commercial cutouts and maintained persistent access through valid credentials after initial exploitation. Review whether your organization appeared in Silk Typhoon targeting scope (COVID-19 research, biotech, defense, government). Update threat model to account for T1591/T1589 pre-compromise reconnaissance. Ensure Exchange is not directly internet-exposed without WAF/IPS as a compensating control per CISA guidance.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel, senior leadership, and potentially CISA (via report@cisa.gov) if historical Exchange IIS log analysis confirms POST requests to /ecp/DDI/ or /owa/auth/Current/ from external IPs during February 2020–June 2021, if unauthorized ASPX files are found in Exchange virtual directories, if mailbox forwarding rules to external domains are discovered, or if the organization falls within Silk Typhoon's documented targeting scope (COVID-19 research, biotech, defense, or federal contractors) — any of these conditions may trigger HIPAA breach notification, FISMA incident reporting, or CIRCIA obligations depending on sector.

Recovery Notes	After eradication is confirmed, restore Exchange to full internet-facing operation only after WAF or reverse proxy (e.g., nginx with ModSecurity) is positioned in front of OWA and ECP endpoints, and only after all Exchange virtual directory configurations have been validated against Microsoft's Exchange Health Checker script output (free tool from Microsoft GitHub). Maintain elevated monitoring of Exchange IIS logs, Windows Security Event IDs 4625/4648/4672, and mailbox delegation changes for a minimum of 90 days post-recovery, given Silk Typhoon's documented use of T1078 (Valid Accounts) for long-duration persistence that survived initial patching cycles during the 2020–2021 campaign. Given the MSS attribution and nation-state TTPs confirmed in the indictment, organizations in targeted sectors should treat any re-emergence of anomalous Exchange authentication patterns as a potential re-entry attempt and re-initiate the full IR lifecycle rather than treating it as routine noise.
Forensic Artifacts	IIS W3SVC1/W3SVC2 log files (C:\inetpub\logs\LogFiles\) spanning February 2020–June 2021: the forensic signature of Silk Typhoon ProxyLogon exploitation is a two-stage unauthenticated POST sequence — first to /ecp/DDI/DDIService.svc/GetObject (CVE-2021-26855 SSRF trigger) followed by a POST to /owa/auth/Current/ or /owa/auth/.aspx (web shell delivery via CVE-2021-27065 OAB virtual directory write), distinguishable from legitimate Exchange traffic by the absence of a valid session cookie in the SSRF request. | Exchange HttpProxy logs (C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\): capture the backend SSRF routing component of CVE-2021-26855 where Hafnium manipulated the X-AnonResource-Backend and X-BEResource cookie headers to authenticate to the backend Exchange endpoint as NT AUTHORITY\SYSTEM — these logs contain the spoofed backend URL values that are absent from standard IIS logs and are the most precise forensic indicator of ProxyLogon exploitation versus other Exchange attack types. | Exchange ECP server logs (C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server\) and CmdletInfra logs (C:\Program Files\Microsoft\Exchange Server\V15\Logging\CmdletInfra\): record the execution of Set-OabVirtualDirectory and New-ExchangeCertificate cmdlets used in CVE-2021-27065 exploitation to write attacker-controlled ASPX content to the OAB virtual directory — these cmdlet audit entries establish the precise timestamp of web shell installation and the Exchange identity under which the commands executed. | NTFS $MFT (Master File Table) and $LogFile from the Exchange server volume: provide byte-level creation and modification timestamps for ASPX files dropped in Exchange virtual directories, enabling timeline reconstruction that distinguishes Silk Typhoon-staged web shells (typically created within minutes of the /ecp/DDI/ log entries) from legitimate Exchange application files — recoverable even if the attacker deleted the ASPX file post-exfiltration using free tools such as Autopsy or Eric Zimmerman's MFTECmd. | Active Directory event logs (Windows Security Event IDs 4720, 4728, 4732, 4738) and Exchange Management Shell audit logs for the 2020–2021 window: Silk Typhoon created local and domain accounts and added them to Exchange role groups (specifically Organization Management) for T1078 persistent access after initial web shell deployment — these event log entries, combined with AD replication metadata (repadmin /showrepl and Get-ADUser with PasswordLastSet/WhenCreated attributes), establish the full persistence timeline beyond the initial exploitation foothold.

Per-Action IR Details

Step 1: Containment — If Exchange Server 2019 or earlier is internet-facing, confirm the December 2025 Exchange security updates are applied (per Microsoft Tech Community blog, December 2025). Verify no web shells remain in IIS virtual directories (OWA, ECP, Autodiscover paths) associated with ProxyLogon/ProxyShell exploitation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose a containment strategy based on criteria such as potential damage, evidence preservation needs, and service availability requirements.

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run Microsoft's Exchange On-Premises Mitigation Tool (EOMT.ps1) — a free, Microsoft-provided script that applies URL rewrite mitigations for ProxyLogon and scans IIS virtual directories for known web shell signatures. Enumerate all ASPX files under Exchange virtual paths with: Get-ChildItem -Recurse -Path 'C:\inetpub\wwwroot\aspnet_client\', 'C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\', 'C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\ecp\' -Filter '*.aspx' | Select FullName, LastWriteTime, Length | Export-Csv webshell_audit.csv. Cross-reference output hashes against known Hafnium web shell hashes published in CISA Alert AA21-062A using Get-FileHash.

Evidence: Before patching or removing files, image or snapshot the Exchange server. Preserve: (1) Full contents of IIS virtual directories — specifically C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ and C:\inetpub\wwwroot\aspnet_client\ — where Hafnium staged web shells such as 'web.aspx', 'healthcheck.aspx', and randomized-name ASPX files post-ProxyLogon exploitation. (2) IIS application pool identity tokens and W3WP.exe process memory dumps if web shell activity is suspected active. (3) Windows NTFS $MFT and $LogFile entries to establish file creation timestamps for any ASPX artifacts, distinguishing attacker-dropped files from legitimate Exchange components. (4) Exchange transport queue database (mail.que) for evidence of data staging or exfiltration via internal mail relay — a documented Hafnium TTPs.

Step 2: Detection — Search Exchange IIS logs (W3SVC1 and W3SVC2) from February 2020 through June 2021 for anomalous POST requests to /owa/auth/Current/, /ecp/DDI/, and /autodiscover/autodiscover.json. Correlate with CISA's Microsoft Exchange Server Security Best Practices advisory for known Hafnium IOC patterns. Use MITRE T1505.003 (web shell) and T1190 (exploitation) as hunting anchors in SIEM.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze all available precursors and indicators, including logs, error messages, and IDS/IPS alerts, correlating them across multiple sources to establish scope.

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

Compensating: Parse Exchange IIS logs (default path: C:\inetpub\logs\LogFiles\W3SVC1\) using PowerShell without a SIEM: Import-Csv -Path (Get-ChildItem 'C:\inetpub\logs\LogFiles\W3SVC1\' -Filter '*.log' | Where-Object {$_.LastWriteTime -gt '2020-02-01' -and $_.LastWriteTime -lt '2021-06-30'}).FullName -Delimiter ' ' | Where-Object {$_.{'cs-uri-stem'} -match '/owa/auth/Current/|/ecp/DDI/|/autodiscover/autodiscover.json' -and $_.{'cs-method'} -eq 'POST'} | Select-Object date, time, 'c-ip', 'cs-uri-stem', 'sc-status' | Export-Csv hafnium_hits.csv. Deploy the free Sigma rule 'win_exchange_proxylogon_webshell' (available in the SigmaHQ repository) against Windows Event Log using Chainsaw (free, Rust-based log scanner) for hosts where IIS logs have been rotated or deleted. Cross-reference source IPs against known Hafnium infrastructure published in CISA AA21-062A and Microsoft MSTIC blog (March 2021).

Evidence: Preserve the following before log rotation overwrites entries: (1) IIS W3SVC1 and W3SVC2 log files spanning February 2020–June 2021 in original format — Hafnium ProxyLogon exploitation produces a distinctive two-stage HTTP pattern: an initial unauthenticated POST to /ecp/DDI/DDIService.svc/GetObject followed by a second POST to /owa/auth/Current/ delivering the web shell payload. (2) Exchange HttpProxy logs at C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\ — these capture backend request routing and reveal the SSRF component of ProxyLogon (CVE-2021-26855) where the attacker spoofed the X-AnonResource-Backend header to reach the backend Exchange endpoint as SYSTEM. (3) Exchange ECP server logs at C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server\ for evidence of unauthorized OAB (Offline Address Book) virtual directory writes, which Hafnium used to stage web shells via CVE-2021-27065. (4) Windows Security Event Log Event ID 4688 (Process Creation) filtered on W3WP.exe spawning cmd.exe, powershell.exe, or certutil.exe — the characteristic pattern of a web shell executing OS commands under the Exchange application pool identity.

Step 3: Eradication — Apply all current Exchange Server security updates per Microsoft's cumulative update cadence. Remove any unauthorized ASPX files from Exchange virtual directories. Rotate credentials for any service accounts with Exchange access; Silk Typhoon used T1078 (Valid Accounts) for persistence after initial access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: After containing the incident, eradicate the cause by deleting malware, disabling breached accounts, and mitigating exploited vulnerabilities to prevent recurrence.

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management) — implied by credential rotation requirement, CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For credential rotation without enterprise PAM tooling: (1) Export all Exchange service accounts via Get-ADServiceAccount -Filter * | Select Name, SamAccountName, LastLogonDate and cross-reference against accounts with Exchange Organization Management or Server Management role group membership via Get-RoleGroupMember. (2) Use the free tool 'BloodHound CE' (community edition) to map which accounts Silk Typhoon may have pivoted through using valid credential reuse — specifically look for accounts that authenticated to Exchange over EWS or MAPI during the 2020–2021 window as captured in Exchange Message Tracking logs. (3) After rotating credentials, deploy YARA rule sets from the CISA AA21-062A advisory against the Exchange installation directory to confirm no residual web shell variants remain before restoring full service.

Evidence: Before credential rotation or file deletion, collect: (1) Active Directory replication metadata for Exchange service accounts — specifically pwdLastSet, LastLogonTimestamp, and adminCount attributes — to establish whether Silk Typhoon elevated privileges using T1078 by modifying account properties rather than resetting passwords, a forensically significant distinction. (2) Exchange Management Shell audit logs at C:\Program Files\Microsoft\Exchange Server\V15\Logging\CmdletInfra\ — Hafnium operators executed Exchange PowerShell cmdlets (New-ExchangeCertificate, Set-OabVirtualDirectory) to reconfigure OAB virtual directories as part of CVE-2021-27065 exploitation; these cmdlet logs capture operator commands with timestamps. (3) Windows Security Event Log Event IDs 4720 (account created), 4732 (member added to security-enabled local group), and 4728 (member added to global security group) for the 2020–2021 window — Silk Typhoon created backdoor accounts for T1078 persistence that may persist in disabled state. (4) LSASS memory dump (using ProcDump: procdump.exe -ma lsass.exe lsass.dmp) if active credential theft is suspected — preserve before credential rotation invalidates the forensic baseline.

Step 4: Recovery — Validate Exchange server integrity against Microsoft's recommended baseline (CISA Exchange Best Practices advisory). Monitor Exchange Application and Security event logs for recurrence of anomalous authentication (Event IDs 4625, 4648, 4672). Confirm no unauthorized forwarding rules or mailbox delegation persists (T1213 indicator).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation, confirm systems are functioning normally, and implement additional monitoring to watch for recurrence of compromise.

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-6 (Security and Privacy Function Verification), CIS 8.2 (Collect Audit Logs), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Audit Exchange mailbox forwarding rules and delegate access without a third-party tool using: (1) Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {$_.ForwardTo -ne $null -or $_.ForwardAsAttachmentTo -ne $null -or $_.RedirectTo -ne $null} | Select MailboxOwnerID, Name, ForwardTo, RedirectTo — Silk Typhoon established forwarding rules to exfiltrate COVID-19 research email to external addresses. (2) Get-MailboxPermission -Identity * | Where-Object {$_.AccessRights -eq 'FullAccess' -and $_.IsInherited -eq $false} to detect unauthorized mailbox delegation added for persistent T1213 collection access. (3) Deploy Sysmon with a configuration tuned to Event ID 3 (Network Connection) filtering on W3WP.exe or UMWorkerProcess.exe making outbound connections to non-Microsoft IP ranges — an indicator of active web shell C2 or data exfiltration resuming post-recovery.

Evidence: Before declaring recovery complete, collect and preserve: (1) Exchange Message Tracking logs (Get-MessageTrackingLog -Start '2020-02-01' -End '2021-06-30' -EventID SEND) filtered for messages sent to external domains from high-value mailboxes — these establish the data exfiltration scope specific to the Silk Typhoon COVID-19 research targeting documented in the indictment. (2) Exchange Mailbox Audit logs (if enabled) from O365 Unified Audit Log or on-premises equivalent, specifically MailboxLogin, SendAs, and MailItemsAccessed operations, which can confirm whether Silk Typhoon accessed specific research mailboxes consistent with their documented targeting of biotech and COVID-19 institutions. (3) Network flow data (NetFlow/IPFIX) for Exchange server outbound connections during the 2020–2021 window — Hafnium exfiltrated data to US-based cloud infrastructure (specifically Vult■ and Choopa VPS providers as documented by Microsoft MSTIC) and this pattern is forensically distinguishable from legitimate Exchange traffic.

Step 5: Post-Incident — This indictment confirms MSS-linked actors use commercial cutouts and maintained persistent access through valid credentials after initial exploitation. Review whether your organization appeared in Silk Typhoon targeting scope (COVID-19 research, biotech, defense, government). Review whether your organization appeared in Silk Typhoon targeting scope (COVID-19 research, biotech, defense, government). Update threat model to account for T1591/T1589 pre-compromise reconnaissance. Ensure Exchange is not directly internet-exposed without WAF/IPS as a compensating control per CISA guidance.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct lessons learned meetings, update IR plans and detection capabilities based on findings, and share threat intelligence to improve the broader community's posture.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment) — implied by threat model update requirement, NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For organizations without enterprise threat intelligence platforms: (1) Subscribe to CISA's free CISA Automated Indicator Sharing (AIS) feed and cross-reference your DNS query logs and firewall egress logs against Silk Typhoon IOCs from AA21-062A and the March 2021 Microsoft MSTIC Hafnium blog post — both are freely available and contain IP ranges and domains used by MSS cutout infrastructure. (2) Use SpiderFoot HX (free community edition) or Maltego CE to assess your organization's external attack surface as Silk Typhoon would have seen it via T1591 reconnaissance — enumerate internet-facing Exchange OWA endpoints, autodiscover DNS records, and certificate transparency logs that would have identified your Exchange version pre-exploitation. (3) Implement ModSecurity (free WAF) with the OWASP CRS ruleset in front of Exchange OWA if a commercial WAF is not available — specifically enable rules targeting SSRF patterns (REQUEST-934-APPLICATION-ATTACK-GENERIC) that would detect ProxyLogon-style X-AnonResource-Backend header manipulation.

Evidence: For the post-incident review, compile and retain: (1) A complete timeline correlating IIS log anomalies, ECP cmdlet audit entries, and AD account modification events — this is the evidentiary foundation for any regulatory notification determination (HIPAA breach notification if COVID-19 research involved PHI; FISMA reporting if the organization is a federal contractor). (2) DNS query logs from the 2020–2021 window for lookups resolving to Hafnium-attributed infrastructure as documented in CISA AA21-062A — passive DNS evidence of pre-exploitation reconnaissance via T1590/T1591 may establish the attacker's dwell time beginning before the first observed IIS log anomaly. (3) Any threat intelligence sharing submissions to CISA's CIRCIA reporting portal or Information Sharing and Analysis Centers (ISACs) relevant to your sector — the Silk Typhoon indictment specifically names biotech, defense, and government verticals, making sector-level intelligence sharing both operationally valuable and potentially required under emerging CIRCIA regulations.

Detection Guidance

Primary hunting surface: Exchange IIS logs from February 2020 through June 2021. Look for POST requests to /owa/auth/Current/themes/resources/, /ecp/DDI/DDIService.svc/, and /autodiscover/ endpoints from external IPs without preceding authenticated sessions, a ProxyLogon pattern. Search for ASPX files created outside normal

Exchange installation paths under %ExchangeInstallPath%FrontEnd\HttpProxy and ClientAccess directories. In Windows Security logs, hunt for Event ID 4624 (Logon Type 3 or 8) from unexpected source IPs against Exchange service accounts. For current threat hunting, map to MITRE T1505.003 (web shell deployment) and T1078 (account reuse) in SIEM. CISA's Microsoft Exchange Server Security Best Practices resource provides detection checkpoints aligned to Hafnium TTP patterns. No new IOCs were released with the indictment; historical Hafnium IOCs from the March 2021 CISA advisory remain the reference set.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not released with indictment`	No new IOCs were published alongside the extradition and indictment. Historical Hafnium IOCs from the March 2021 CISA and Microsoft disclosures remain the reference set. Consult CISA's Exchange advisory for the current IOC list.	LOW

Framework Mappings

MITRE-ATTACK

- **T1505.003** — Web Shell
- **T1560** — Archive Collected Data
- **T1591** — Gather Victim Org Information
- **T1059** — Command and Scripting Interpreter
- **T1588.006** — Vulnerabilities
- **T1071** — Application Layer Protocol
- **T1589** — Gather Victim Identity Information
- **T1078** — Valid Accounts
- **T1213** — Data from Information Repositories
- **T1583.001** — Domains
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **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
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

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

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

ISO-27001-2022

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

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
T1505.003	Web Shell	Persistence
T1560	Archive Collected Data	Collection

Technique ID	Technique Name	Tactic
T1591	Gather Victim Org Information	Reconnaissance
T1059	Command and Scripting Interpreter	Execution
T1588.006	Vulnerabilities	Resource-Development
T1071	Application Layer Protocol	Command-And-Control
T1589	Gather Victim Identity Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1583.001	Domains	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/chinese-silk-typhoon-hacker-extra...	T3
Description of the security update for Microsoft Exchange Server 2019	https://support.microsoft.com/en-us/topic/description-of-the-securi...	T1
Microsoft Exchange Server Security Best Practices - CISA	https://www.cisa.gov/resources-tools/resources/microsoft-exchange-s...	T1
Microsoft Exchange Server security vulnerabilities, CVEs, versions ...	https://www.cvedetails.com/product/194/Microsoft-Exchange-Server.ht...	T3
Released: December 2025 Exchange Server Security Updates	https://techcommunity.microsoft.com/blog/exchange/released-december...	T1

Generated 2026-04-28 18:50 UTC by TJS Security Command Center