INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 19:30 UTC

June 2026 Patch Tuesday: 200 Vulnerabilities Including Three Zero-Days Across Windows, Office, and Azure

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0277
Type	CVE Vulnerability
CVE ID	CVE-2026-45586, CVE-2026-49160, CVE-2026-50507, CVE-2026-45491, CVE-2026-45490, CVE-2026-45648, CVE-2026-45591, CVE-2026-47643, CVE-2026-41098, CVE-2026-42836, CVE-2026-45482, CVE-2026-45476, CVE-2026-45642, CVE-2026-33828, CVE-2026-32193, CVE-2026-45650, CVE-2026-45647, CVE-2026-40371, CVE-2026-45500, CVE-2026-45501, CVE-2026-47631, CVE-2026-45503, CVE-2026-45504, CVE-2026-45502, CVE-2026-45583, CVE-2026-42986, CVE-2026-41092, CVE-2026-45644, CVE-2026-45463, CVE-2026-44821, CVE-2026-45474, CVE-2026-44819, CVE-2026-44824, CVE-2026-45485, CVE-2026-45645, CVE-2026-45472, CVE-2026-45458, CVE-2026-45460, CVE-2026-47635, CVE-2026-45456, CVE-2026-45461, CVE-2026-45475, CVE-2026-47293, CVE-2026-44820, CVE-2026-44818, CVE-2026-44817
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Windows 11, Windows 10, Windows Server 2022/2025, Microsoft Office (Word, Excel, Outlook), Microsoft Exchange Server, Azure Stack Edge, Azure Kubernetes Service, Microsoft Defender for Endpoint, .NET, ASP.NET Core, HTTP.sys, BitLocker, Windows Active Directory Domain Services, Microsoft Dynamics 365, Microsoft Bing, Visual Studio Code, GitHub Copilot
Published	2026-06-09T13:57:59
Discovery Source	Rss

Executive Summary

Microsoft's June 2026 Patch Tuesday resolves 200 vulnerabilities across Windows, Office, Exchange Server, Azure, and developer tooling, including three publicly disclosed zero-days rated Critical. The zero-days cover privilege escalation, a BitLocker encryption bypass, and an HTTP/2 denial-of-service vector affecting Windows Server infrastructure. As of patch release, no confirmed exploitation in the wild has been reported, but public disclosure ahead of patching narrows the window before weaponized exploits emerge.

Technical Analysis

Microsoft released patches for 200 CVEs on June 2026 Patch Tuesday, with 33 rated Critical and a peak CVSS base score of 9.5 assigned to the highest-severity privilege escalation vulnerability. Three zero-days were publicly disclosed prior to patch availability: a privilege escalation flaw (MITRE T1548, T1068, T1134), a BitLocker security feature bypass (CWE-693, MITRE T1542, T1553) that may allow an attacker to circumvent full-volume encryption protections, and an HTTP/2 denial-of-service vector (CWE-400, MITRE T1499) in HTTP.sys affecting Windows Server. CWE-59 (link following/symlink abuse) is present across at least one component, consistent with T1574 (hijack execution flow). Two zero-days were disclosed publicly prior to patch availability by an independent security researcher, compressing the patching window ahead of standard Microsoft disclosure practices. Affected surface includes Windows 10/11, Windows Server 2022/2025, Microsoft Office (Word, Excel, Outlook), Exchange Server, Azure Stack Edge, Azure Kubernetes Service, Microsoft Defender for Endpoint, .NET, ASP.NET Core, HTTP.sys, BitLocker, Active Directory Domain Services, Dynamics 365, Bing, Visual Studio Code, and GitHub Copilot. No CISA KEV listing as of patch release date; EPSS scores not yet populated. Key CVEs in scope include CVE-2026-45586, CVE-2026-49160, CVE-2026-50507, and 43 additional identifiers across the full advisory set (comprehensive CVE list available in MSRC June 2026 Patch Tuesday advisory). Sources: MSRC advisory set (T1), BleepingComputer June 2026 Patch Tuesday coverage (T3), Zero Day Initiative June 2026 Security Update Review (T3).

Action Checklist

1. Step 1: Containment, Prioritize patching internet-facing Windows Server systems running HTTP.sys immediately; the HTTP/2 DoS zero-day (CWE-400, T1499) can be triggered remotely and may disrupt production services. Temporarily restrict external HTTP/2 traffic at the perimeter WAF or load balancer if patching cannot begin within 24 hours. For BitLocker bypass (CWE-693, T1542/T1553), assess which endpoints use BitLocker without pre-boot authentication and consider enabling TPM+PIN as interim mitigation. Reference the MSRC June 2026 Patch Tuesday advisory for affected build numbers before scoping patch deployment. Map to NIST SI-4 (system monitoring) and CIS 7.1 (vulnerability management process).
2. Step 2: Detection, Query endpoint management tooling (SCCM, Intune, or equivalent) for unpatched Windows 10/11 and Server 2022/2025 builds predating June 2026 cumulative updates. For the privilege escalation zero-days (T1548, T1068, T1134), review Windows Security event logs for Event ID 4672 (special privilege logon), 4688 (process creation with elevated tokens), and 4697 (service installation) on endpoints that have not yet received the patch. For HTTP.sys DoS indicators, monitor IIS/HTTP.sys logs for malformed HTTP/2 frame sequences or unexpected worker process crashes. For BitLocker bypass, check BitLocker management logs for unexpected recovery key access events (Event ID 24658 in Microsoft-Windows-BitLocker-API/Management). Apply CIS 8.2 (collect audit logs) and NIST AU-6 (audit record review and analysis) to ensure log collection is active across affected asset classes. No confirmed IOCs are available at this time; detection relies on patch gap identification and behavioral anomalies.
3. Step 3: Eradication, Deploy June 2026 cumulative updates from the MSRC update guide to all affected platforms in priority order: (1) internet-facing Windows Server running HTTP.sys, (2) Active Directory domain controllers (privilege escalation scope), (3) Exchange Server, (4) all Windows 10/11 endpoints. For Office suite (Word, Excel, Outlook), deploy via Microsoft Update or M365 Admin Center. For Azure Stack Edge and AKS, follow Microsoft's cloud service update notifications, some components update automatically. For .NET and ASP.NET Core, redeploy applications targeting patched runtime versions.

Reference CIS 7.3 (automated OS patch management) and CIS 7.4 (automated application patch management).

4. Step 4: Recovery, After deploying updates, validate patch application via endpoint management reporting and confirm June 2026 KB numbers are present on all in-scope systems. Run a targeted vulnerability scan scoped to CVEs in this advisory to confirm closure. Re-enable any temporarily restricted HTTP/2 traffic only after patch confirmation. For BitLocker-protected endpoints, verify BitLocker status has not changed post-patch using 'manage-bde -status' or equivalent tooling. Monitor Windows Security event logs for 72 hours post-patch for any residual privilege escalation indicators (Event IDs 4672, 4688). Apply NIST AU-6 (audit record review) and CIS 8.2 (audit log collection) to post-patch monitoring. Document patch completion dates for compliance records.

5. Step 5: Post-Incident, Conduct a lessons-learned review focused on three control gaps this advisory exposed: (a) patch deployment velocity for zero-days with public disclosure ahead of vendor release, assess whether your patching SLA covers this scenario and update CIS 7.2 (remediation process) documentation accordingly; (b) BitLocker configuration standards, review whether all endpoints enforce pre-boot authentication per NIST AC-3 (access enforcement) and CIS 3.6 (encrypt data on end-user devices); (c) HTTP/2 exposure surface, verify perimeter controls align with NIST AC-4 (information flow enforcement) and CIS 4.4/4.5 (firewall management).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance if Event ID 24658 (BitLocker recovery key access) or Event ID 773 (BitLocker unlocked via recovery password) is observed on endpoints containing PII or PHI prior to patch completion, or if Event IDs 4672/4697 indicate a new privileged account or service was created on a DC or Exchange server during the public disclosure window, as either condition suggests active exploitation rather than patch gap exposure and may trigger breach notification obligations.
Recovery Notes	Re-enable restricted HTTP/2 traffic only after confirming the June 2026 cumulative update KB is present on all internet-facing Windows Server systems via `Get-HotFix` validation — do not rely solely on SCCM compliance reports, as WMI reporting lag can show false compliance. Maintain heightened monitoring on Active Directory for new privileged account creation and on Exchange ECP/OWA logs for anomalous access for a minimum of 72 hours post-patch across all tiers, extending to 7 days for DCs given the privilege escalation zero-day scope. BitLocker-protected endpoints should be re-audited for protector integrity one week post-patch to confirm no recovery key substitution occurred silently during the vulnerability window.

Forensic Artifacts	Windows Security Event Log (Security.evtx) on domain controllers and Exchange servers: filter Event IDs 4672 (special privilege logon), 4688 (process creation), 4697 (service installation), and 4698 (scheduled task creation) for the period spanning June 2026 Patch Tuesday public disclosure through patch completion — these are the primary behavioral indicators for T1548/T1068/T1134 privilege escalation exploitation of the Windows zero-days. | Microsoft-Windows-BitLocker-API/Management event log on all BitLocker-enabled endpoints: Event ID 24658 (recovery key accessed) and Event ID 773 (volume unlocked with recovery password) would be the direct forensic signature of CVE-2026-45648 or related BitLocker bypass (CWE-693, T1542/T1553) exploitation, indicating an attacker defeated pre-boot protection. | IIS/HTTP.sys W3SVC logs at `%SystemRoot%\System32\LogFiles\W3SVC*` on all internet-facing Windows Server instances: look for HTTP/2 SETTINGS frame floods, RST_STREAM storms, or patterns of w3wp.exe worker process recycling (cross-reference Application Event Log ID 1000/1026) that would be consistent with remote CWE-400 resource exhaustion exploitation of the HTTP.sys DoS zero-day (T1499). | Active Directory audit logs via `Get-ADObject -Filter * -SearchBase (Get-ADDomain).DistinguishedName -Properties WhenCreated,WhenChanged | Where-Object {$_.WhenCreated -gt [datetime]'2026-06-01'}` to detect new accounts, group membership changes to privileged groups (Domain Admins, Enterprise Admins), or GPO modifications created after public zero-day disclosure — these would indicate post-disclosure exploitation of the privilege escalation zero-days before patching completed. | Sysmon Event ID 10 (process access) and Event ID 8 (CreateRemoteThread) logs on unpatched Windows 10/11 and Server 2022/2025 hosts, filterable via `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational'` for source processes targeting lsass.exe or winlogon.exe — these would capture in-memory exploitation artifacts consistent with T1134 (Access Token Manipulation) exploitation of the privilege escalation zero-days prior to patch deployment.

Per-Action IR Details

Step 1: Containment — Prioritize patching internet-facing Windows Server systems running HTTP.sys immediately; the HTTP/2 DoS zero-day (CWE-400, T1499) can be triggered remotely and may disrupt production services. Temporarily restrict external HTTP/2 traffic at the perimeter WAF or load balancer if patching cannot begin within 24 hours. For BitLocker bypass (CWE-693, T1542/T1553), assess which endpoints use BitLocker without pre-boot authentication and consider enabling TPM+PIN as interim mitigation. Reference MSRC advisory set for affected build numbers before scoping patch deployment. Map to NIST SI-4 (system monitoring) and CIS 7.1 (vulnerability management process).

NIST Phase: Containment

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without a WAF appliance, use Windows Firewall to block inbound HTTP/2 (TCP 443 with ALPN h2) on exposed IIS servers via PowerShell: `New-NetFirewallRule -DisplayName 'Block HTTP2 Inbound' -Direction Inbound -Protocol TCP -LocalPort 443 -Action Block` — note this will also block standard HTTPS until scoped by IP allowlist. For BitLocker TPM+PIN enforcement without MDM, run `manage-bde -protectors -add C: -TPMAndPIN` on each at-risk endpoint. Use `manage-bde -status` across the fleet via a PSRemoting loop to identify endpoints with TPM-only protection.

Evidence: Before implementing WAF blocks or TPM+PIN changes, capture: (1) current IIS/HTTP.sys configuration from `%SystemRoot%\System32\inetsrv\config\applicationHost.config` to document pre-containment HTTP/2 enablement state; (2) BitLocker protector inventory via `manage-bde -protectors -get C:` on all endpoints to establish which systems had TPM-only protection before any mitigation; (3) Windows System Event Log for Event ID 7036

(service state change) and Event ID 7031 (service crash) on HTTP.sys-dependent services to establish a crash baseline prior to any traffic restriction.

Step 2: Detection — Query endpoint management tooling (SCCM, Intune, or equivalent) for unpatched Windows 10/11 and Server 2022/2025 builds predating June 2026 cumulative updates. For the privilege escalation zero-days (T1548, T1068, T1134), review Windows Security event logs for Event ID 4672 (special privilege logon), 4688 (process creation with elevated tokens), and 4697 (service installation) on endpoints that have not yet received the patch. For HTTP.sys DoS indicators, monitor IIS/HTTP.sys logs in %SystemRoot%\System32\LogFiles\W3SVC* for malformed HTTP/2 frame sequences or unexpected worker process crashes. For BitLocker bypass, check BitLocker management logs for unexpected recovery key access events (Event ID 24658 in Microsoft-Windows-BitLocker-API/Management). Apply CIS 8.2 (collect audit logs) and NIST AU-6 (audit record review and analysis) to ensure log collection is active across affected asset classes. No confirmed IOCs are available at this time; detection relies on patch gap identification and behavioral anomalies.

NIST Phase: Detection Analysis

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

Controls: AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs), AU-2 (Event Logging), AU-12 (Audit Record Generation)

Compensating: Without SIEM, deploy Sysmon with SwiftOnSecurity config to capture process creation and token privilege events on unpatched hosts. Run the following PowerShell to extract privilege escalation candidates on unpatched endpoints: `Get-WinEvent -LogName Security -FilterXPath "*[System[(EventID=4672 or EventID=4688 or EventID=4697)]]" | Where-Object { $_.TimeCreated -gt (Get-Date).AddDays(-3) } | Export-Csv C:\IR\priv_events.csv`. For HTTP.sys crash detection without EDR, configure a scheduled task to monitor W3WP process crashes via Event ID 1000 in the Application log and alert via email using Send-MailMessage. For BitLocker, parse Microsoft-Windows-BitLocker-API/Management log on all endpoints using `wevtutil qe Microsoft-Windows-BitLocker-API/Management /f:text /q:"*[System[EventID=24658]]"` piped to a central share.

Evidence: Before concluding detection scope, preserve: (1) Windows Security event logs (Security.evtx) from all unpatched hosts covering the period from June 2026 Patch Tuesday release date forward, specifically filtered for Event IDs 4672, 4688, 4697, and 4698 (scheduled task creation); (2) IIS logs from `%SystemRoot%\System32\LogFiles\W3SVC*` on internet-facing servers for HTTP/2 SETTINGS frame floods or RST_STREAM anomalies indicative of CWE-400 resource exhaustion exploitation attempts against CVE-2026-45583 or related HTTP.sys CVEs; (3) Microsoft-Windows-BitLocker-API/Management event log exports for Event ID 24658 (recovery key access) and Event ID 773 (BitLocker volume unlocked with recovery password) which would indicate exploitation of the BitLocker bypass zero-day.

Step 3: Eradication — Deploy June 2026 cumulative updates from the MSRC update guide (https://msrc.microsoft.com/update-guide) to all affected platforms in priority order: (1) internet-facing Windows Server running HTTP.sys, (2) Active Directory domain controllers (privilege escalation scope), (3) Exchange Server, (4) all Windows 10/11 endpoints. For Office suite (Word, Excel, Outlook), deploy via Microsoft Update or M365 Admin Center. For Azure Stack Edge and AKS, follow Microsoft's cloud service update notifications — some components update automatically. For .NET and ASP.NET Core, redeploy applications targeting patched runtime versions. Reference CIS 7.3 (automated OS patch management) and CIS 7.4 (automated application patch management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Without SCCM or Intune, use PSWindowsUpdate PowerShell module (`Install-WindowsUpdate -AcceptAll -AutoReboot`) executed via PSRemoting against a prioritized host list — sequence: HTTP.sys servers first, then DCs, then Exchange, then endpoints. For Office patching without M365 Admin Center push, use the Office Deployment Tool (ODT) with `/update user` switch against a local UNC share hosting the June 2026 channel update. For .NET runtime verification, run `dotnet --list-runtimes` on each app server and compare against Microsoft's published patched runtime versions for June 2026; redeploy from dotnet.microsoft.com if unpatched runtimes are found.

Evidence: Before patching each tier, snapshot: (1) running process list (`Get-Process` output) and loaded driver list (`driverquery /fo csv`) on each DC and Exchange server to detect any pre-patch compromise artifacts such as unusual services or drivers that could persist post-patch — specifically look for unsigned kernel drivers that could be associated with T1068 local privilege escalation exploitation; (2) Active Directory for any new accounts, group membership changes, or GPO modifications created within 72 hours of public zero-day disclosure using `Get-ADUser -Filter * -Properties Created | Where-Object {$_.Created -gt [datetime]'2026-06-01'}` and `Get-ADGroupMember 'Domain Admins'` baseline comparison; (3) Exchange transport logs and OWA/ECP access logs from `%ExchangeInstallPath%\Logging` for anomalous authentication or privilege use prior to patch deployment.

Step 4: Recovery — After deploying updates, validate patch application via endpoint management reporting and confirm June 2026 KB numbers are present on all in-scope systems. Run a targeted vulnerability scan scoped to CVEs in this advisory to confirm closure. Re-enable any temporarily restricted HTTP/2 traffic only after patch confirmation. For BitLocker-protected endpoints, verify BitLocker status has not changed post-patch using 'manage-bde -status' or equivalent tooling. Monitor Windows Security event logs for 72 hours post-patch for any residual privilege escalation indicators (Event IDs 4672, 4688). Apply NIST AU-6 (audit record review) and CIS 8.2 (audit log collection) to post-patch monitoring. Document patch completion dates for compliance records.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs), AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a vulnerability scanner license, use Microsoft's free MSRC-published detection scripts or run `Get-HotFix -Id ` via PSRemoting across all hosts to confirm KB presence; export results to CSV for compliance documentation. For HTTP/2 re-enablement validation, test with curl: `curl --http2 -v https://` from an external vantage point and confirm 200 responses without service disruption. For BitLocker post-patch integrity, script `manage-bde -status` across all endpoints and diff against the pre-patch baseline captured in Step 1 to detect any protector changes introduced during patching.

Evidence: During the 72-hour post-patch monitoring window, collect and retain: (1) Windows Security event logs filtered for Event IDs 4672, 4688, and 4697 on DCs and Exchange servers to detect any privilege escalation activity that may indicate pre-patch compromise now surfacing post-remediation; (2) BitLocker-API/Management event log for Event IDs 773 and 24658 post-patch to confirm no recovery key access occurred during or after the update process, which could indicate the bypass was exploited during the patch window; (3) IIS/HTTP.sys W3SVC logs for the first 24 hours after HTTP/2 traffic is re-enabled to establish a clean post-patch baseline and detect any retry exploitation attempts against previously exposed servers.

Step 5: Post-Incident — Conduct a lessons-learned review focused on three control gaps this advisory exposed: (a) patch deployment velocity for zero-days with public disclosure ahead of vendor release — assess whether your patching SLA covers this scenario and update CIS 7.2 (remediation process) documentation accordingly; (b) BitLocker configuration standards — review whether all endpoints enforce pre-boot authentication per NIST AC-3 (access enforcement) and CIS 3.6 (encrypt data on end-user devices); (c) HTTP/2 exposure surface — verify perimeter controls align with NIST AC-4 (information flow enforcement) and CIS 4.4/4.5 (firewall management). Additionally, review your researcher disclosure intake process; the Nightmare Eclipse incident reflects a coordinated disclosure breakdown that could affect future patch

timelines.

NIST Phase: Post Incident

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

Controls: CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.6 (Encrypt Data on End-User Devices), AC-3 (Access Enforcement), AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without a formal GRC platform, document lessons learned in a structured markdown template covering: (a) time-to-patch metric for each priority tier against your SLA, calculated from June 2026 Patch Tuesday release date; (b) BitLocker TPM-only endpoint count identified in Step 1 as the gap metric driving pre-boot auth remediation; (c) HTTP/2 exposure surface documented as a list of public-facing IPs with h2 enabled pre-patch, sourced from the firewall rule audit in Step 1. Store this as a dated artifact in your IR case file. Use the osquery query `SELECT * FROM bitlocker_info` for ongoing BitLocker posture monitoring without MDM tooling.

Evidence: For the lessons-learned record, assemble the following artifacts specific to this advisory cycle: (1) patch velocity report showing time-delta between June 2026 Patch Tuesday publication and confirmed KB installation per priority tier (HTTP.sys servers, DCs, Exchange, endpoints) — this directly measures SLA adequacy for publicly disclosed zero-days; (2) BitLocker protector inventory diff between pre-containment baseline (Step 1) and post-recovery validation (Step 4) to quantify endpoints that had TPM-only protection and were remediated to TPM+PIN; (3) HTTP/2 exposure surface documentation including pre-patch firewall rule state, duration of HTTP/2 restriction, and post-patch re-enablement timestamps to support both internal review and any regulatory compliance documentation requirements.

Detection Guidance

No confirmed IOCs are available for this advisory as of the patch release date; none of the three zero-days are listed in the CISA KEV catalog, and EPSS scores are not yet populated. Detection must focus on patch gap identification and behavioral anomalies consistent with the vulnerability classes present. For privilege escalation (T1548, T1068, T1134): query Windows Security event logs for Event ID 4672 (special privilege assigned), 4688 (new process with elevated token), and 4697 (service installed) on unpatched Windows 10/11 and Server 2022/2025 systems. For the BitLocker bypass (CWE-693, T1542/T1553): monitor Microsoft-Windows-BitLocker-API/Management log (Event ID 24658) for unexpected recovery key access, and review TPM event logs for anomalous unlock sequences. For the HTTP/2 DoS vector (CWE-400, T1499): monitor HTTP.sys and IIS logs for malformed or oversized HTTP/2 HEADERS/DATA frames, and alert on unexpected w3wp.exe or http.sys crashes (Windows Application/System log, Event Source: HTTP, W3SVC). For CWE-59 (symlink/link following): enable object access auditing (NIST AU-2, AU-12) and monitor for unexpected symbolic link creation events in sensitive directories (Event ID 4663 with ObjectType: Symbolic Link). Patch gap scanning via SCCM, Intune, or a vulnerability scanner filtered to June 2026 KB identifiers is the highest-confidence detection method at this stage. Apply NIST AU-6 and CIS 8.2 controls to ensure log coverage is active across all affected asset classes.

Framework Mappings

MITRE-ATTACK

- **T1574** — Hijack Execution Flow
- **T1553** — Subvert Trust Controls
- **T1499** — Endpoint Denial of Service
- **T1203** — Exploitation for Client Execution

- **T1200** — Hardware Additions
- **T1190** — Exploit Public-Facing Application
- **T1548** — Abuse Elevation Control Mechanism
- **T1068** — Exploitation for Privilege Escalation
- **T1134** — Access Token Manipulation
- **T1542** — Pre-OS Boot

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **IR-5** — Incident Monitoring

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

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

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1574	Hijack Execution Flow	Persistence
T1553	Subvert Trust Controls	Defense-Evasion

Technique ID	Technique Name	Tactic
T1499	Endpoint Denial of Service	Impact
T1203	Exploitation for Client Execution	Execution
T1200	Hardware Additions	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1134	Access Token Manipulation	Defense-Evasion
T1542	Pre-OS Boot	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2026...	T3
The June 2026 Security Update Review - Zero Day Initiative	https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-secur...	T3
CVE-2026-34334 - Microsoft Security Response Center (MSRC)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34334	T1
CVE-2026-1973 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-1973	T1
CVE-2026-45891 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-45891	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-45586, CVE-2026-49160, CV...	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-4558...	T1

Generated 2026-06-09 19:30 UTC by TJS Security Command Center