INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-18 13:45 UTC

Ivanti, Fortinet, SAP, VMware, and n8n Release Security Patches for RCE, SQL Injection, and Privilege Escalation Vulnerabilities

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0143
Type	Security Analysis
Severity	HIGH
Affected Products	Ivanti (unspecified products), Fortinet (unspecified products), SAP (unspecified products), VMware (unspecified products), n8n (workflow automation platform)
Published	6 hours ago
Discovery Source	Serper

Executive Summary

Five enterprise vendors, Ivanti, Fortinet, SAP, VMware, and n8n, released security patches in a coordinated disclosure cycle addressing remote code execution, SQL injection, authentication bypass, and privilege escalation vulnerabilities across network appliances, business applications, virtualization infrastructure, and workflow automation tooling. The breadth of affected vendor categories means most organizations carry exposure across at least one affected product line. Given historical rapid weaponization of Ivanti and Fortinet vulnerabilities, the window between disclosure and active exploitation is typically narrow (days to weeks), compressing the timeframe for response. Security teams should treat this as a multi-front patching event requiring immediate inventory and prioritization rather than routine maintenance. IMPORTANT: This story is sourced from social media aggregation and does not include vendor advisory URLs or specific CVE identifiers. Before executing the action plan below, retrieve authoritative patch notices directly from vendor PSIRT channels to confirm which specific CVE IDs, affected versions, and patch availability apply to your environment.

Technical Analysis

This disclosure cycle spans five distinct vendor ecosystems, each carrying different attacker value and exploitation pathways. The vulnerability classes present, CWE-287 (authentication bypass), CWE-89 (SQL injection), CWE-269 (privilege escalation), and CWE-78 (OS command injection), map directly to three high-value MITRE ATT&CK techniques: T1190 (Exploit Public-Facing Application), T1059 (Command and

Scripting Interpreter), and T1068 (Exploitation for Privilege Escalation). This combination represents a near-complete initial access and post-exploitation chain.

Ivanti and Fortinet network appliances sit at the perimeter, making their vulnerabilities particularly high-value for initial access. Both vendors have sustained histories of actively exploited zero-days and n-days; Ivanti and Fortinet have maintained entries on CISA's Known Exploited Vulnerabilities (KEV) catalog in recent years, establishing baseline attacker interest in these vendors. SAP business applications hold sensitive financial and HR data, making authentication bypass and SQL injection in that environment a direct path to data exfiltration or business process manipulation. VMware virtualization infrastructure, if compromised via privilege escalation, can expose entire compute environments across guest systems. n8n, a workflow automation platform with broad API integration capabilities, represents a lower-profile but high-consequence target; if the disclosed vulnerability permits privilege escalation or RCE within the workflow runtime, a compromised automation node could be weaponized to execute commands or API calls using credentials stored in workflow configuration - a lateral movement path often overlooked in patch prioritization.

Exploitation status is unconfirmed from available source data. However, the historical pattern for Ivanti and Fortinet vulnerabilities specifically is rapid weaponization following disclosure, often within days. Source data for this story is limited to social media references; full CVE identifiers, CVSS scores, affected version ranges, and vendor advisory links are not available in the provided material. Security teams must consult vendor advisories directly for authoritative patch scope and applicability confirmation.

Action Checklist

1. Step 0 (CRITICAL): Retrieve vendor advisories before proceeding. This story is sourced from social media aggregation. Pull official patch notices from: Ivanti PSIRT (psirt.ivanti.com), Fortinet PSIRT (fortinet.com/psirt), SAP Security Patch Day (support.sap.com/securitypatchday), VMware Security Advisories (vmware.com/security), and n8n Security (github.com/n8n-io/n8n/security/advisories). Confirm specific CVE IDs, affected versions, and patch availability before assigning response timelines.
2. Step 1: Assess exposure. Inventory all instances of Ivanti (network appliances, VPN gateways, endpoint management), Fortinet (FortiOS-based security appliances), SAP (ERP, S/4HANA, Business Suite), VMware (vSphere, ESXi, vCenter), and n8n (self-hosted or cloud workflow automation) across production, staging, and DMZ environments. Cross-reference against CVE IDs from vendor advisories.
3. Step 2: Prioritize Ivanti and Fortinet perimeter systems. Both vendors have documented rapid exploitation histories and KEV catalog entries. Authentication bypass (CWE-287) and OS command injection (CWE-78) on internet-facing appliances warrant immediate patching or compensating controls (network segmentation, emergency firewall policy, emergency WAF rules if applicable).
4. Step 3: Assess patch availability and timelines. If patches are not yet available from vendors, implement compensating controls and request vendor ETA. Do not assume patches are available for all affected products; some vendors may stage releases.
5. Step 4: Review controls relevant to post-exploitation TTPs. Verify EDR coverage on systems adjacent to patched appliances, audit privileged account access on VMware infrastructure, and review n8n service account permissions for least-privilege compliance.
6. Step 5: Update threat model and vulnerability register. Add each vendor and CVE ID (once confirmed via advisories) to your vulnerability register with owner assignments, SLA timelines, and escalation triggers if patches cannot be applied within your defined window for high-severity findings.

7. Step 6: Monitor for exploitation indicators. Track CISA KEV catalog updates and Ivanti and Fortinet PSIRT feeds for active exploitation confirmation; set alerting on anomalous authentication events and command execution logs on affected systems.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to incident status if CISA adds any CVE from this patch cycle to the KEV catalog, if anomalous authentication events are detected on Ivanti or Fortinet perimeter appliances during the unpatched window, if VMware vCenter shows unexpected role modifications or snapshot activity, or if your organization is subject to NERC CIP, HIPAA, or PCI-DSS and affected systems are in scope — all of which carry breach notification obligations if exploitation is confirmed.
Recovery Notes	After patching Ivanti and Fortinet appliances, force-terminate all active VPN and SSL-VPN sessions and require re-authentication to prevent session token hijacking that may have occurred during the exposure window — this is specifically relevant to authentication bypass (CWE-287) class vulnerabilities. For VMware, after applying privilege escalation patches, audit all vCenter roles and permissions for unauthorized modifications and rotate service account credentials used by vCenter and ESXi. Monitor all patched systems for at least 30 days post-patch using the log sources identified in Step 6, with specific attention to re-emergence of the indicator patterns documented pre-patch, as threat actors with existing footholds may persist through the patch cycle.
Forensic Artifacts	Ivanti Connect Secure '/data/runtime/logs/log.events' and '/data/runtime/logs/debuglog': authentication bypass exploitation (CWE-287) against Ivanti appliances historically produces anomalous session establishment entries, unexpected admin endpoint access, and malformed authentication header patterns — archive these logs with cryptographic hash before any patch or reboot wipes volatile entries | Fortinet FortiGate system event logs ('Log & Report > Events > System Events') filtered for daemon-level process execution and admin configuration changes: OS command injection (CWE-78) exploitation would manifest as web process spawning unexpected child processes (e.g., shell, Python, wget) visible in FortiOS process audit logs if process-level logging is enabled | VMware vCenter '/var/log/vmware/vpxd/vpxd.log' and ESXi '/var/log/hostd.log': privilege escalation exploitation would leave traces of unexpected role assignments, new local account creation, VM snapshot creation (a common persistence/exfil technique), or vCenter API calls authenticated with anomalous session tokens | n8n execution database ('~/.n8n/database.sqlite' for self-hosted instances): RCE exploitation via workflow automation would appear as unexpected workflow executions, particularly those invoking the 'Execute Command' node or making outbound HTTP requests to attacker-controlled infrastructure — query the execution_entity table for all executions in the 30 days preceding the advisory | Active Directory Security Event Log Event IDs 4728/4732/4756 (security group membership changes) and 4720 (new account creation) on domain controllers: post-exploitation of authentication bypass on Ivanti VPN gateways commonly results in immediate lateral movement and credential abuse visible as anomalous group membership changes correlating in time to the appliance exploitation window

Per-Action IR Details

Step 1: Assess exposure — inventory all instances of Ivanti (network appliances, VPN gateways), Fortinet (firewalls, FortiOS-based products), SAP (ERP, S/4HANA, Business Suite), VMware (vSphere, ESXi, vCenter), and n8n (self-hosted or cloud workflow automation) across production, staging, and DMZ environments

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and maintain asset visibility prior to incident declaration

Controls: NIST IR-4 (Incident Handling) — preparation sub-requirement for maintaining asset inventories, NIST SI-5 (Security Alerts, Advisories, and Directives) — act on vendor advisories by first establishing affected asset scope, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must include network appliances, virtualization hosts, ERP instances, and SaaS/self-hosted automation tooling, CIS 2.2 (Ensure Authorized Software is Currently Supported) — confirm all Ivanti, Fortinet, SAP, VMware, and n8n versions in inventory are still vendor-supported and patchable

Compensating: Run 'nmap -sV -p 443,8443,4443,8080 ' against DMZ and perimeter ranges to fingerprint Ivanti ZTNA/Connect Secure and Fortinet FortiGate management interfaces. For internal VMware: 'nmap -p 443,902,903 ' to locate vCenter and ESXi hosts. For n8n: grep Apache/Nginx access logs for '/rest/workflows' or '/webhook/' URI patterns to locate self-hosted instances. Cross-reference against your CMDB or a quick 'aws ec2 describe-instances' / 'az vm list' for cloud-hosted appliances.

Evidence: Before inventorying, snapshot current DHCP lease tables and DNS A-record exports so you have a point-in-time record of what was reachable at advisory publication — this establishes your exposure window baseline. For Fortinet appliances, capture 'get system status' output via console before patching to document exact FortiOS build strings. For VMware, export vCenter inventory via 'Get-VM | Select Name,Version,PowerState | Export-CSV' (PowerCLI) to record ESXi host versions pre-patch.

Step 2: Pull vendor advisories directly — source data for this story is limited to social media and a paywalled article; retrieve official patch notices from Ivanti PSIRT, Fortinet PSIRT, SAP Security Patch Day, VMware Security Advisories, and the n8n GitHub security advisories for authoritative CVE IDs and affected versions

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Maintain access to authoritative threat intelligence sources as a precondition for accurate triage

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — designate Ivanti PSIRT, Fortinet PSIRT, SAP Security Patch Day, and VMware Security Advisories as required external advisory feeds, NIST IR-8 (Incident Response Plan) — IR plan must identify authoritative vendor sources to prevent triage errors caused by incomplete third-party reporting, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability process must gate patching decisions on official CVE IDs and affected version ranges, not secondary reporting

Compensating: Subscribe to Ivanti PSIRT RSS (https://www.ivanti.com/blog/security-advisories), Fortinet PSIRT RSS, and SAP Security Notes via the SAP Support Portal. For n8n, watch the GitHub repo Security Advisories tab ('github.com/n8n-io/n8n/security/advisories'). Use a free RSS aggregator (Feedly free tier or tt-rss self-hosted) to consolidate these into a single monitoring queue. Without a formal vuln management platform, maintain a shared spreadsheet mapping CVE IDs to asset IDs pulled from Step 1, updated each time an official advisory is released.

Evidence: Archive the raw vendor advisory pages (PDF print or wget) at time of retrieval with a timestamp — this creates a dated record of what was publicly known and when, which is essential if regulatory notification timelines are later scrutinized. Note: without confirmed CVE IDs from official advisories, CVSS scoring and KEV correlation cannot be performed accurately; do not initiate SLA timers until official CVE IDs are in hand.

Step 3: Prioritize Ivanti and Fortinet perimeter systems — both vendors have recent KEV catalog entries and documented rapid exploitation histories; authentication bypass (CWE-287) and OS command injection (CWE-78) on internet-facing appliances warrant immediate patching or compensating controls (WAF rules, network segmentation, emergency firewall policy)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Apply compensating controls when patches cannot be immediately deployed to limit attacker dwell time on perimeter systems

Controls: NIST IR-4 (Incident Handling) — containment actions for internet-facing appliances with active exploitation history must be treated as incident-level response, not standard patching, NIST SI-2 (Flaw Remediation) — test and apply vendor patches; where immediate patching is not possible, document compensating controls and residual risk,

NIST SC-7 (Boundary Protection) — enforce network segmentation to isolate Ivanti VPN gateways and Fortinet perimeter devices from internal trust zones pending patch application, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation process must assign highest priority tier to internet-facing appliances with CWE-287/CWE-78 and KEV catalog presence, CIS 4.4 (Implement and Manage a Firewall on Servers) — restrict management interface access on Fortinet and Ivanti appliances to dedicated jump hosts or management VLANs

Compensating: For Fortinet: use 'config system interface / set allowaccess' to restrict management GUI/SSH to a dedicated management IP only; disable internet-facing admin access via CLI. For Ivanti Connect Secure/ZTNA: disable external-facing admin portal access and enforce client certificate requirements if not patched. Deploy a free ModSecurity WAF rule (OWASP Core Rule Set) upstream if your architecture permits. For OS command injection (CWE-78), create an ACL on your perimeter router/switch blocking direct internet access to appliance management ports (TCP 443/8443/SSH) from any source except your management VLAN — achievable with a two-line ACL on most enterprise switches.

Evidence: Before applying compensating controls, capture: (1) Fortinet FortiGate event logs from 'Log & Report > Events > System Events' filtered for admin login attempts and configuration changes in the past 30 days — export as CSV; (2) Ivanti Connect Secure debug logs from '/data/runtime/logs/debuglog' for authentication events and any anomalous URI patterns indicative of authentication bypass attempts (e.g., malformed header injection, path traversal in login endpoints); (3) NetFlow or firewall session logs showing all source IPs that reached the management interface in the past 14 days — this establishes whether exploitation attempts preceded your compensating controls.

Step 4: Review controls relevant to post-exploitation TTPs — verify EDR coverage on systems adjacent to patched appliances, audit privileged account access on VMware infrastructure, and review n8n service account permissions for least-privilege compliance

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate post-exploitation indicators across systems adjacent to vulnerable appliances; do not limit analysis to the patched device itself

Controls: NIST SI-4 (System Monitoring) — extend monitoring to systems that authenticate through or are managed by vulnerable Ivanti VPN gateways and Fortinet appliances, as these are lateral movement targets post-authentication bypass, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review VMware vCenter audit logs and n8n execution logs for privilege escalation indicators consistent with post-exploitation of the underlying vulnerabilities, NIST IR-5 (Incident Monitoring) — track and document all anomalous privileged access events on VMware vCenter and ESXi hosts that could indicate exploitation of VMware privilege escalation CVEs in this cycle, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — audit VMware vCenter role assignments and n8n instance owner/admin roles; remove any over-privileged service accounts, CIS 6.3 (Require MFA for Externally-Exposed Applications) — verify MFA enforcement on n8n webhook endpoints and VMware vCenter if internet-accessible

Compensating: For VMware without enterprise EDR: enable vCenter audit logging ('Administration > System Configuration > Syslog') and forward to a free syslog server (rsyslog or syslog-ng). Query ESXi host auth logs at '/var/log/auth.log' and '/var/log/shell.log' for unexpected root shell activity. For n8n: review the execution log database (SQLite at '~/.n8n/database.sqlite' for self-hosted instances) with 'sqlite3 database.sqlite "SELECT * FROM execution_entity WHERE startedAt > datetime(\"now\", \"-7 days\");"' to identify unexpected workflow executions. For EDR gap on adjacent Linux hosts: deploy osquery with the 'processes', 'logged_in_users', and 'socket_events' tables to catch post-exploitation process spawning.

Evidence: For VMware privilege escalation post-exploitation: capture vCenter '/var/log/vmware/vpxd/vpxd.log' and ESXi '/var/log/hostd.log' for unexpected VM snapshot creation, vCenter role modification events, or new local account creation — these are common post-exploitation persistence actions. For n8n: if the RCE vulnerability targets the workflow automation engine, capture all files created or modified under the n8n working directory (default '~/.n8n/') in the past 30 days using 'find ~/.n8n -newer /tmp/baseline_timestamp -ls'. For Ivanti/Fortinet post-auth-bypass: check Active Directory logs for new service account creations or group membership changes (Event ID 4728, 4732, 4756) correlating to the exploitation window.

Step 5: Update threat model — add this multi-vendor patch cycle to your vulnerability register with owner assignments, SLA timelines, and escalation triggers if patches cannot be applied within your defined window

for high-severity findings

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Update policies, detection capabilities, and risk register based on lessons learned and emerging threat intelligence

Controls: NIST IR-8 (Incident Response Plan) — update IR plan to include escalation procedures specific to multi-vendor coordinated patch cycles that compress remediation windows across product categories simultaneously, NIST RA-3 (Risk Assessment) — formally document residual risk for any Ivanti, Fortinet, SAP, VMware, or n8n instance that cannot be patched within SLA; require risk acceptance sign-off from system owner, NIST SI-2 (Flaw Remediation) — enforce documented SLA timelines for high-severity flaws; internet-facing appliances with CWE-287 or CWE-78 and KEV catalog status should carry a 24-72 hour patch SLA, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability register entries for this cycle must include: CVE ID (once confirmed from Step 2), affected asset IDs, owner, patch SLA, compensating control status, and escalation trigger date, CIS 7.2 (Establish and Maintain a Remediation Process) — assign explicit ownership for each vendor track (Ivanti, Fortinet, SAP, VMware, n8n); multi-vendor cycles fail remediation SLAs when ownership is diffuse

Compensating: Maintain the vulnerability register in a shared spreadsheet or free Jira/GitHub Issues project with columns: CVE ID, vendor, affected asset hostname/IP, owner, patch-by date, compensating control applied (Y/N), escalation date. Set a recurring calendar reminder at 50% and 90% of the SLA window to check patch status. For escalation triggers without a formal GRC tool: use a simple cron job or free Zapier/n8n (ironic, but applicable) webhook to notify the security lead when the patch-by date is 48 hours away and the 'patched' field is still blank.

Evidence: Before closing out the vulnerability register entries, preserve: the original vendor advisory text and publication timestamp (from Step 2), the compensating control configuration snapshots (firewall ACL exports, Fortinet 'show full-configuration' output), and the asset inventory state from Step 1. These form the audit trail demonstrating due diligence if a regulatory inquiry arises after a breach involving one of these CVEs.

Step 6: Monitor for exploitation indicators — track CISA KEV catalog updates and Ivanti and Fortinet PSIRT feeds for active exploitation confirmation; set alerting on anomalous authentication events and command execution logs on affected systems before patches are applied

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Establish monitoring for known exploitation indicators on vulnerable systems during the patch gap window

Controls: NIST SI-4 (System Monitoring) — implement targeted monitoring on Ivanti and Fortinet management interfaces and authentication endpoints during the unpatched window; treat any anomalous authentication as a potential exploitation attempt, NIST AU-2 (Event Logging) — ensure logging is enabled and capturing authentication events, command execution, and configuration changes on all in-scope appliances before exploitation indicators emerge, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review logs from affected Ivanti VPN/ZTNA and Fortinet FortiOS systems at increased frequency (minimum daily, ideally continuous) until patched, NIST IR-6 (Incident Reporting) — establish a clear internal reporting path: if CISA adds a new Ivanti or Fortinet CVE from this cycle to the KEV catalog, immediately escalate from monitoring to active incident investigation, CIS 8.2 (Collect Audit Logs) — confirm audit logging is active and log forwarding is functioning on all Ivanti, Fortinet, VMware, and n8n instances before the exploitation window widens

Compensating: For Ivanti Connect Secure: monitor '/data/runtime/logs/log.events' for HTTP 4xx spikes against '/dana-na/auth/' endpoints and anomalous User-Agent strings — known exploitation of past Ivanti CVEs (e.g., CVE-2024-21887) produced distinctive URI patterns. For Fortinet: use the free FortiGate built-in syslog to forward 'event_type=login' and 'event_type=system' log classes to a remote rsyslog server; write a Sigma rule detecting failed-then-succeeded authentication sequences within 60 seconds from the same source IP. Deploy a free Sysmon configuration (SwiftOnSecurity ruleset) on Windows hosts adjacent to these appliances to catch post-exploitation process injection (Event ID 8) or unusual parent-child process relationships (Event ID 1) indicating lateral movement from a compromised appliance. Use 'tail -f' with grep on Fortinet and Ivanti log files as a manual poor-man's SIEM if no aggregation is available.

Evidence: Pre-patch, capture and timestamp: (1) Ivanti Connect Secure '/data/runtime/logs/log.events' and '/data/runtime/logs/debuglog' — authentication bypass exploits against Ivanti historically produce anomalous session

token generation entries and unexpected POST requests to admin endpoints; (2) Fortinet FortiGate 'execute log filter' output for all admin authentication events and firewall policy modification events from the past 14 days — OS command injection (CWE-78) exploitation would appear as unexpected system-level commands executed under the web process or daemon context; (3) Windows Security Event Log Event ID 4648 (explicit credential logon) and Event ID 4624 (logon type 3, network) on systems that authenticate through the Ivanti VPN gateway — these are the earliest host-side indicators of credential abuse following authentication bypass.

Detection Guidance

Given the vulnerability classes disclosed, focus detection on three behavioral patterns. First, for authentication bypass (CWE-287) on Ivanti and Fortinet appliances: review VPN and firewall authentication logs for successful logins from unexpected source IPs, unusual time-of-day access, or sessions without corresponding MFA events. Baseline normal authentication patterns now, before exploitation is confirmed. Second, for SQL injection (CWE-89) in SAP environments: enable or review SAP application-layer logging for abnormal database query patterns, particularly SELECT statements with unusual WHERE clause structures or queries targeting user/credential tables. Third, for privilege escalation (CWE-269) in VMware: monitor vCenter and ESXi audit logs for unexpected role assignments, new admin account creation, or API calls from non-standard service accounts. For n8n specifically, audit workflow execution logs for unexpected external HTTP requests, credential access events, or newly created workflows with elevated permissions. MITRE T1190 hunting: if web application firewall (WAF) is deployed on appliance management interfaces, correlate WAF logs against patch disclosure dates - a spike in structured error responses or HTTP 500s is a strong indicator of active scanning or exploitation attempts. Organizations without WAF on management interfaces should monitor firewall access logs for repeated failed authentication attempts or unusual source IPs against appliance management ports (typically 8443, 8080, or 22 depending on vendor) post-disclosure.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Pending — refer to Ivanti PSIRT advisories (https://www.ivanti.com/blog/security-update) for published CVE IDs and indicators`	Ivanti PSIRT publishes affected version ranges and indicators; specific CVE values not available in source data	LOW
URL	`Pending — refer to Fortinet PSIRT advisories (https://www.fortiguard.com/psirt) for published CVE IDs and indicators`	Fortinet PSIRT advisories include affected FortiOS versions, CVSS scores, and available workarounds; specific values not available in source data	LOW
URL	`Pending — refer to SAP Security Patch Day bulletin (https://support.sap.com/en/my-support/security-notes.html) for published notes and CVSS scores`	SAP Security Patch Day notes include affected product versions and SQL injection/authentication advisory details; specific values not available in source data	LOW

Type	Value	Context	Confidence
URL	`Pending — refer to VMware Security Advisories (https://www.vmware.com/security/advisories.html) for published CVE IDs`	VMware advisories include privilege escalation CVE details and affected vSphere/ESXi/vCenter versions; specific values not available in source data	LOW
URL	`Pending — refer to n8n GitHub Security Advisories (https://github.com/n8n-io/n8n/security/advisories) for published vulnerability details`	n8n publishes RCE and related security advisories on GitHub; specific CVE values and affected versions not available in source data	LOW

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **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-6** — Least Privilege
- **SI-10** — Information Input Validation
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **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
- **2.5** — Allowlist Authorized Software
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
	https://thehackernews.com/2026/05/ivanti-fortinet-sap-vmware-n8n-pa...	T3
Ivanti, Fortinet, SAP, VMware and n8n released fixes for flaws tied to ...	https://x.com/TheHackersNews/status/2056327606732247200	T3

Source	URL	Tier
Ivanti, Fortinet, SAP, VMware and n8n released fixes for flaws tied to ...	https://www.instagram.com/p/DYekrdjviVJ/	T3
The Hacker - Ivanti, Fortinet, SAP, VMware and n8n released fixes ...	https://www.facebook.com/thehackernews/photos/-ivanti-fortinet-sap-...	T3
Ivanti, Fortinet, SAP, VMware, n8n Patch RCE, SQL ... - Reddit	https://www.reddit.com/r/SecOpsDaily/comments/1tgkkve/ivanti_fortin...	T3

Generated 2026-05-18 13:45 UTC by TJS Security Command Center