INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-18 06:14 UTC

47 Zero-Days in 3 Days: Pwn2Own Berlin 2026 Exposes Critical Gaps Across Microsoft, VMware, and Red Hat Enterprise Stacks

SECURITY ANALYSIS | CRITICAL | CVSS 9.5

SCC Item ID	SCC-STY-2026-0141
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft Exchange, Microsoft Windows 11, Microsoft Edge, Microsoft SharePoint, VMware ESXi, Red Hat Enterprise Linux for Workstations, NVIDIA Container Toolkit
Published	2026-05-18T01:33:20
Discovery Source	Rss

Executive Summary

Pwn2Own Berlin 2026 produced 47 confirmed zero-day vulnerabilities across Microsoft Exchange, Windows 11, VMware ESXi, Red Hat Enterprise Linux, and NVIDIA Container Toolkit in three days, yielding $1,298,250 in researcher payouts and signaling material unpatched risk across the enterprise stack. The most consequential finding was a three-bug chain delivering SYSTEM-level remote code execution on Microsoft Exchange, a platform with a well-documented history of rapid weaponization after public disclosure. Security teams now operate inside a 90-day coordinated disclosure window before technical details become available to the broader threat landscape, including ransomware operators and nation-state actors.

Technical Analysis

Pwn2Own Berlin 2026 concluded May 2026 with six research teams, DEVCORE, STARLabs SG, IBM X-Force Offensive Research, Viettel Cyber Security, Summoning Team, and Out Of Bounds, demonstrating 47 zero-days across a concentrated set of enterprise-critical platforms. The competition's structure requires live exploitation under controlled conditions, making each confirmed finding a validated, weaponizable attack path rather than a theoretical vulnerability.

The headline finding was a chained exploit against Microsoft Exchange combining three discrete vulnerabilities to achieve SYSTEM-level remote code execution. Exchange's relevance here extends beyond the technical: following ProxyLogon (CVE-2021-26855) and ProxyShell (CVE-2021-34473), threat actors have consistently

converted Exchange disclosures into active exploitation within days of public details emerging. A SYSTEM-level RCE chain on Exchange represents the most dangerous class of finding at this competition, and defenders should treat the 90-day ZDI embargo as a hard countdown.

Vulnerability classes observed across the competition span use-after-free (CWE-416), integer overflow (CWE-190), memory corruption (CWE-119), and code injection (CWE-94), all well-understood primitive classes with a long history of chaining into privilege escalation and lateral movement. The MITRE ATT&CK techniques mapped to demonstrated exploits include T1203 (Exploitation for Client Execution), T1059 (Command and Scripting Interpreter), T1068 (Exploitation for Privilege Escalation), T1210 (Exploitation of Remote Services), T1611 (Escape to Host), T1548 (Abuse Elevation Control Mechanism), T1190 (Exploit Public-Facing Application), and T1078 (Valid Accounts), a profile consistent with initial access, escalation, and container escape chains.

The inclusion of VMware ESXi and NVIDIA Container Toolkit as confirmed targets carries specific implications for virtualization and AI/ML infrastructure. ESXi exploitation enabling container escape (T1611) directly threatens hypervisor-level isolation in environments where multiple tenants or workloads share physical hardware. The NVIDIA Container Toolkit findings extend this risk to GPU-accelerated workloads, which increasingly underpin AI inference pipelines and sensitive data processing. Emerging infrastructure platforms were demonstrated as exploitable at this event, marking a notable expansion of the competition's scope.

Red Hat Enterprise Linux for Workstations appearing in the confirmed target list is relevant for organizations that treat Linux endpoints as inherently lower-risk than Windows environments, a posture this competition's results directly challenge.

The 90-day ZDI disclosure window is the critical operational variable. Zero-days demonstrated at Pwn2Own are under coordinated disclosure: vendors receive technical details and are expected to patch before ZDI publishes. However, historical precedent shows that motivated threat actors sometimes reverse-engineer patches and develop exploits faster than enterprise patch cycles permit. Security teams should not treat the embargo as a guarantee of safe deferral.

Action Checklist

1. Step 1: Assess exposure, inventory all deployments of Microsoft Exchange (on-premises), Windows 11, VMware ESXi, Red Hat Enterprise Linux for Workstations, and NVIDIA Container Toolkit. If your organization runs Microsoft Edge or SharePoint in adjacent or dependent infrastructure, verify coverage separately; cloud-hosted Exchange Online requires separate confirmation from Microsoft on shared-responsibility scope.
2. Step 2: Review controls, verify compensating controls for Exchange specifically: network egress restrictions from Exchange servers, EDR coverage with memory protection enabled, privileged access workstations for Exchange administration, and monitoring on Exchange-related processes (w3wp.exe, UMWorkerProcess.exe) for anomalous behavior.
3. Step 3: Update threat model, add SYSTEM-level RCE via chained Exchange vulnerabilities to your threat register; map T1203, T1068, T1210, and T1611 to existing detection coverage and identify gaps, particularly for ESXi container escape and NVIDIA Container Toolkit abuse paths.
4. Step 4: Communicate findings, brief leadership on the Exchange finding specifically, using the ProxyLogon/ProxyShell precedent to frame time-to-exploitation risk; note that the 90-day embargo does not mean zero exploitation risk during that window.

5. Step 5: Monitor developments, subscribe to ZDI advisories (zerodayinitiative.com), Microsoft Security Response Center (MSRC), VMware Security Advisories, and Red Hat Security Advisories; establish a patch SLA for any CVEs assigned from this competition that affect your environment, treating Exchange RCE findings as P1.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and initiate formal incident response if any of the following are observed: (1) w3wp.exe or UMWorkerProcess.exe spawning interactive shells or making unexpected outbound connections on Exchange servers, (2) new web shells detected in Exchange virtual directories (IIS paths under `%ExchangeInstallPath%\FrontEnd\HttpProxy`), (3) evidence of container escape from NVIDIA Container Toolkit or ESXi environments to host-level access, (4) SIEM or Sysmon alerts correlating T1210/T1068/T1611 activity across Exchange and adjacent systems, or (5) if Exchange servers hold PII or PHI and any anomalous access is detected, triggering breach notification assessment under applicable regulations (HIPAA §164.402, GDPR Art. 33).
Recovery Notes	After any Exchange patching or remediation, verify integrity of all files in Exchange virtual directories — specifically `/owa/`, `/ecp/`, `/autodiscover/`, `/mapi/`, and `/rpc/` — using a known-good file hash baseline, as post-exploitation web shells planted during the embargo window would persist through patching if not explicitly hunted (consistent with ProxyLogon incident patterns where shells survived patching). Monitor Exchange IIS logs and Sysmon process creation events for a minimum of 30 days post-patch for anomalous w3wp.exe or UMWorkerProcess.exe behavior, as actors with pre-patch access may have established persistence via scheduled tasks or registry run keys. For ESXi, revalidate VM isolation boundaries post-patch by auditing host-level API call logs in `/var/log/hostd.log` and confirming no unauthorized persistent jobs exist via `vim-cmd vimsvc/task_list`.

Forensic Artifacts	Exchange IIS W3C access logs (`%SystemDrive%\inetpub\logs\LogFiles\W3SVC1\`) — a three-bug Exchange RCE chain would produce anomalous HTTP requests to /autodiscover/, /ecp/, /owa/, or /mapi/ endpoints with unusual user-agents, crafted headers, or large POST bodies; compare against baseline from Step 1 to identify pre-patch exploitation attempts during the embargo window | Sysmon Event ID 1 (Process Create) on Exchange servers — exploitation of Exchange RCE would manifest as w3wp.exe (IIS worker) or UMWorkerProcess.exe spawning cmd.exe, powershell.exe, or a renamed binary; Event ID 3 (Network Connection) would show these processes initiating unexpected outbound connections to attacker-controlled infrastructure | Exchange virtual directory file system artifacts — post-exploitation web shell deployment (consistent with ProxyLogon/ProxyShell attack patterns) would leave ASPX or ASHX files in `%ExchangeInstallPath%\FrontEnd\HttpProxy\owa\auth\` or similar IIS-accessible paths; use `Get-ChildItem -Path 'C:\inetpub\wwwroot' -Recurse -Filter *.aspx | Where-Object {$_.LastWriteTime -gt (Get-Date).AddDays(-30)}` to identify recently modified web-accessible files | VMware ESXi `/var/log/vmkernel.log` and `/var/log/hostd.log` — an ESXi container escape (T1611) would produce kernel-level log entries reflecting unauthorized VM-to-host boundary crossing, unexpected privileged API calls, or abnormal datastore access patterns; these logs must be preserved before ESXi patches are applied as they may be rotated | NVIDIA Container Toolkit abuse artifacts — container escape via NVIDIA Container Toolkit would leave traces in host-level Linux audit logs (`/var/log/audit/audit.log`) as syscalls from a container process operating with unexpected host filesystem or device access; use `ausearch -m syscall -ts today | grep -E 'mount|open|write' | grep -v 'success=no'` filtered to container process PIDs to identify unauthorized host interactions

Per-Action IR Details

Step 1: Assess exposure — inventory all deployments of Microsoft Exchange (on-premises), Windows 11, Microsoft Edge, Microsoft SharePoint, VMware ESXi, Red Hat Enterprise Linux for Workstations, and NVIDIA Container Toolkit; cloud-hosted Exchange Online requires separate confirmation from Microsoft on shared-responsibility scope

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability requires knowing what assets exist and their exposure before an incident occurs

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires asset awareness to scope response, NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and act on advisories from ZDI and MSRC for these specific products, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must capture Exchange version, CU level, and whether OWA/ECP are internet-facing, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — documented process must address zero-day exposure windows before CVE assignment

Compensating: Run `Get-ExchangeServer | Select Name, Edition, AdminDisplayVersion` via Exchange Management Shell to enumerate all on-prem Exchange servers and CU levels. For ESXi, use `esxcli system version get` over SSH on each host. For NVIDIA Container Toolkit, run `dpkg -l nvidia-container-toolkit` (Debian/Ubuntu) or `rpm -qa | grep nvidia-container` (RHEL). Document results in a spreadsheet with columns: hostname, product, version, internet-facing (Y/N), last patch date. For Windows 11 scope, query Active Directory with `Get-ADComputer -Filter {OperatingSystem -like '*Windows 11*'} | Select Name,OperatingSystem,OperatingSystemVersion`.

Evidence: Before any remediation, snapshot the current state: export Exchange server IIS logs from `%SystemDrive%\inetpub\logs\LogFiles\W3SVC1` for the prior 30 days to establish a clean baseline of normal request patterns against /owa/, /ecp/, /autodiscover/, /mapi/, and /rpc/ endpoints — these are the URI paths exploited in Exchange RCE chains (ProxyLogon used /ecp/ stage-one, ProxyShell used /autodiscover/). Capture ESXi host profiles via `vim-cmd hostsvc/firmware/backup_config` before any changes.

Step 2: Review controls — verify compensating controls for Exchange specifically: network egress restrictions from Exchange servers, EDR coverage with memory protection enabled, privileged access workstations for Exchange administration, and monitoring on Exchange-related processes (w3wp.exe, UMWorkerProcess.exe) for anomalous behavior

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for adversary techniques targeting known-vulnerable components; CSF DE.CM-09 directs monitoring of computing hardware and software for potentially adverse events

Controls: NIST SI-4 (System Monitoring) — monitor Exchange IIS worker process (w3wp.exe) and UMWorkerProcess.exe for anomalous child process spawning indicative of RCE exploitation, NIST AU-2 (Event Logging) — ensure process creation, network connection, and PowerShell script block logging are enabled on Exchange servers, NIST AU-12 (Audit Record Generation) — Exchange servers must generate audit records capturing IIS request headers, source IPs, and HTTP response codes, CIS 4.4 (Implement and Manage a Firewall on Servers) — Exchange servers should have host-based firewall rules blocking outbound connections on non-standard ports from w3wp.exe, CIS 8.2 (Collect Audit Logs) — IIS logs, Windows Security event logs, and PowerShell operational logs must be collected from Exchange servers

Compensating: Deploy Sysmon with SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) on all Exchange servers; Event ID 1 (Process Create) will capture w3wp.exe or UMWorkerProcess.exe spawning cmd.exe, powershell.exe, or net.exe. Enable PowerShell Script Block Logging via GPO: `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging` → `EnableScriptBlockLogging=1`. Enable Windows Firewall outbound rules to block Exchange service accounts from initiating connections to external IPs on ports other than 25/443/80. Use the free Sigma rule `win_susp_shell_spawn_from_iis.yml` converted to Windows Event Log queries to detect IIS-spawned shells without a SIEM.

Evidence: Capture Sysmon Event ID 3 (Network Connection) showing w3wp.exe or UMWorkerProcess.exe initiating outbound connections — Exchange RCE chains (consistent with the Pwn2Own three-bug pattern) would show the IIS worker process making unexpected outbound connections post-exploitation. Also collect Windows Security Event Log Event ID 4688 (Process Creation with command line) on Exchange servers, filtered to parent processes `w3wp.exe` and `UMWorkerProcess.exe` — a web shell or RCE payload would manifest as cmd.exe, powershell.exe, or a renamed binary spawned by these parent processes.

Step 3: Update threat model — add SYSTEM-level RCE via chained Exchange vulnerabilities to your threat register; map T1203, T1068, T1210, and T1611 to existing detection coverage and identify gaps, particularly for ESXi container escape and NVIDIA Container Toolkit abuse paths

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Threat modeling and detection gap analysis are pre-incident activities that directly reduce time-to-detect when exploitation occurs

Controls: NIST RA-3 (Risk Assessment) — formally document SYSTEM-level RCE on Exchange as a high-risk scenario given ProxyLogon/ProxyShell weaponization precedent (sub-72-hour exploitation after disclosure), NIST IR-4 (Incident Handling) — incident handling capability must address the specific attack patterns: chained Exchange bugs (T1210 Exploitation of Remote Services), privilege escalation to SYSTEM (T1068), ESXi container escape (T1611 Escape to Host), NIST SI-7 (Software, Firmware, and Information Integrity) — integrity monitoring on Exchange binaries and ESXi host configuration to detect post-exploitation tampering, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — threat register update and ATT&CK technique mapping must feed into vuln management prioritization

Compensating: Use the free ATT&CK Navigator (attack.mitre.org/resources/attack-navigator) to create a layer mapping T1203 (Exploitation for Client Execution — Edge/SharePoint browser-side bugs), T1068 (Exploitation for Privilege Escalation — Windows 11 and RHEL LPE bugs), T1210 (Exploitation of Remote Services — Exchange RCE chain), and T1611 (Escape to Host — ESXi and NVIDIA Container Toolkit escapes) against your existing detection controls. For NVIDIA Container Toolkit container escapes specifically, query running containers with `docker inspect --format='{{.HostConfig.Privileged}}' $(docker ps -q)` to identify privileged containers that would be highest-risk targets. For ESXi, audit enabled APIs with `esxcli system settings advanced list | grep -i api`.

Evidence: Prior to updating the threat model, preserve current detection rule state: export existing SIEM correlation rules or Sigma rules covering process injection, named pipe impersonation, and container breakout — document which ATT&CK techniques currently have no detection coverage. For ESXi container escape forensics, the artifact trail would include VMware `/var/log/vmkernel.log` and `/var/log/hostd.log` showing unexpected VM escape operations or privileged API calls; capture these baseline logs before threat model updates alter monitoring configuration.

Step 4: Communicate findings — brief leadership on the Exchange finding specifically, using the ProxyLogon/ProxyShell precedent to frame time-to-exploitation risk; note that the 90-day embargo does not mean zero exploitation risk during that window

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Leadership communication and stakeholder alignment on risk posture are preparation activities; CSF GV functions require governance-level awareness of material risk

Controls: NIST IR-6 (Incident Reporting) — reporting structure must include upward communication of high-severity pre-incident risk, not only active incidents, NIST IR-8 (Incident Response Plan) — IR plan must have a pre-patch notification path for critical zero-day findings affecting high-value systems like Exchange, NIST SI-5 (Security Alerts, Advisories, and Directives) — dissemination of ZDI/MSRC advisories to management is a required activity under this control, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation strategy must be communicated to decision-makers who authorize emergency change windows

Compensating: Prepare a one-page risk brief quantifying the ProxyLogon/ProxyShell precedent: ProxyLogon (CVE-2021-26855) was weaponized within 2 days of public PoC; ProxyShell (CVE-2021-34473) had public PoC-to-mass-exploitation in under 5 days. Frame the current finding as: three-bug Exchange RCE chain demonstrated at Pwn2Own, embargo period active, weaponization likely within days of CVE publication. Include the number of internet-facing Exchange servers from Step 1 inventory and estimated blast radius (number of mailboxes, presence of sensitive data). No specialized tools needed — this is a structured narrative brief using documented historical precedent.

Evidence: Before briefing leadership, collect supporting data that quantifies organizational exposure: (1) count of Exchange servers with OWA/ECP accessible from the internet (check firewall logs or run `nmap -p 443 --script http-title ` to confirm exposed endpoints), (2) Exchange server patching lag from Step 1 inventory showing current CU level versus latest available CU, and (3) any historical IDS/WAF alerts on Exchange endpoints over the past 90 days that may indicate pre-embargo reconnaissance activity against /owa/, /ecp/, or /autodiscover/ paths.

Step 5: Monitor developments — subscribe to ZDI advisories (zerodayinitiative.com), Microsoft Security Response Center (MSRC), VMware Security Advisories, and Red Hat Security Advisories; establish a patch SLA for any CVEs assigned from this competition that affect your environment, treating Exchange RCE findings as P1

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Intelligence integration and process improvement to prevent recurrence; CSF DE.AE-07 directs integration of CTI into adverse event analysis on an ongoing basis

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formal subscription to ZDI, MSRC, VMware, and Red Hat advisory feeds with defined internal SLA for triage and action, NIST IR-4 (Incident Handling) — incident handling process must incorporate advisory-driven patch SLAs; Exchange RCE = P1 (patch within 24-48 hours of CVE publication based on ProxyLogon/ProxyShell precedent), NIST SI-2 (Flaw Remediation) — test and deploy patches for Exchange RCE, ESXi escape, and NVIDIA Container Toolkit findings within P1 SLA; document exceptions with compensating controls, CIS 7.3 (Perform Automated Operating System Patch Management) — automated patch management must be configured to prioritize Exchange Cumulative Updates and Windows 11 security updates tied to Pwn2Own findings, CIS 7.4 (Perform Automated Application Patch Management) — VMware ESXi patches, RHEL errata, and NVIDIA Container Toolkit updates must be tracked and applied under the same P1 SLA

Compensating: Configure RSS feed subscriptions for: ZDI (feeds.feedburner.com/ZDIAdvisories — verify this resolves before use; labeled as search-retrieved, validate manually), MSRC (msrc.microsoft.com/update-guide/rss), VMware Security Advisories (via vmware.com/security/advisories RSS), and Red Hat CVE feed (access.redhat.com/security/updates/advisory). Use a free tool like FreshRSS (self-hosted) or a shared Slack channel

with RSS-to-webhook integration to route advisories directly to the security team. For patch SLA tracking without a ticketing system, maintain a shared spreadsheet with columns: CVE, product, CVSS, advisory date, patch available date, patch applied date, delta (days). Flag any Exchange RCE CVE assigned from Pwn2Own Berlin 2026 competition findings as P1 requiring patch within 48 hours of patch availability.

Evidence: Establish a monitoring baseline before CVEs are assigned: capture current Exchange HTTP access logs (IIS W3C format from `%SystemDrive%\inetpub\logs\LogFiles\`) and configure log archival so you have clean pre-CVE traffic patterns to diff against post-CVE traffic for anomaly detection. For VMware ESXi, preserve `/var/log/esxi_install.log` and `/var/log/vmkernel.log` baselines. When CVEs are formally assigned from this competition, immediately query these logs retroactively for exploitation indicators — threat actors with pre-embargo access to vulnerability details (common in Pwn2Own contexts where multiple researchers may hold similar findings) may have already begun probing.

Detection Guidance

During the embargo period, no technical indicators from the demonstrated exploits are public. Detection posture should focus on behavioral anomalies consistent with the MITRE techniques mapped to this competition.

For Microsoft Exchange (on-premises): Monitor for unexpected child processes spawned by IIS worker processes (w3wp.exe) or Exchange backend services. Alert on SYSTEM-level process creation from Exchange application pools. Review IIS logs for anomalous POST request patterns to Exchange OWA, EWS, and Autodiscover endpoints, the same telemetry that surfaced ProxyLogon and ProxyShell activity. Flag any new scheduled tasks, services, or registry run keys created in the context of Exchange service accounts.

For VMware ESXi: Alert on unexpected process execution at the hypervisor level, particularly processes spawned outside normal administrative workflows. Monitor for container-to-host escape indicators: processes running outside expected namespaces, unexpected privileged container activity, and filesystem access patterns inconsistent with container workload profiles (T1611).

For NVIDIA Container Toolkit: Review container runtime logs for privilege escalation attempts. Monitor GPU process namespacing for anomalies indicating escape attempts from containerized workloads.

For Windows 11 and Red Hat Enterprise Linux endpoints: Ensure EDR telemetry covers memory allocation anomalies associated with use-after-free and integer overflow exploitation (heap spray patterns, unusual memory region execution). Audit local privilege escalation paths (T1068, T1548) and verify Secure Boot and kernel integrity protections are active.

Log sources to prioritize: Windows Security Event Log (4688 process creation with command line), Sysmon (Event IDs 1, 10, 25), IIS access logs for Exchange, ESXi shell audit logs, container runtime logs (containerd, Docker daemon), and Linux auditd for RHEL endpoints.

When CVEs are assigned and patches release, review patch changelogs and MSRC/vendor advisories for behavioral clues. However, do not assume patch diffs will reveal exploitable detail before ZDI publication. Prioritize EDR-based behavioral detection of the MITRE techniques mapped above (T1203, T1068, T1210, T1611) rather than relying on patch-derived indicators during the embargo period.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Zero Day Initiative (zerodayinitiative.com) advisories for published indicators post-embargo`	Technical exploit details, payload hashes, and any network indicators from demonstrated exploits are under 90-day coordinated disclosure embargo; ZDI will publish full advisories upon embargo expiration or vendor patch release	LOW

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1210** — Exploitation of Remote Services
- **T1611** — Escape to Host
- **T1548** — Abuse Elevation Control Mechanism
- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-6** — Configuration Settings
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

OWASP-TOP10-2021

- **A03:2021** — Injection

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
T1203	Exploitation for Client Execution	Execution
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1210	Exploitation of Remote Services	Lateral-Movement
T1611	Escape to Host	Privilege-Escalation
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hackers-earn-1-298-2...	T3
	https://www.bleepingcomputer.com/news/security/hackers-earn-1-298-2...	T3
	https://www.bleepingcomputer.com/news/security/pwn2own-day-two-hack...	T3
Pwn2Own Berlin 2026, Day One: $523,000 paid out, AI products fall	https://securityaffairs.com/192183/hacking/pwn2own-berlin-2026-day-...	T3
Hackers Earn Nearly $400,000 for New Zero-Days at Pwn2Own ...	https://hackyourmom.com/en/novyny/hakery-zarobyly-majzhe-400-tysyac...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-18 06:14 UTC by TJS Security Command Center