Incident Response Playbook: Critical Vulnerabilities & Patch Management

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Monthly for critical advisories / Quarterly otherwise
Approver	CISO / Head of IR

Contents

1 Introduction

1.1 Purpose

This playbook defines response procedures for incidents related to **Critical Vulnerabilities & Patch Management**, with emphasis on **Zero-Day Exploit Detection** and emergency patch coordination. It supports SOC analysts, vulnerability management teams, IT operations, change control, legal and leadership to rapidly assess risk, contain exploitation, and coordinate mitigations and patching.

1.2 Scope

Covers discovery and exploitation of critical vulnerabilities in on-premise systems, cloud workloads, network devices, third-party applications, libraries (SBOM/OSS), and container images. Includes vulnerability triage, emergency change-control, coordination with vendors and patch rollouts.

2 Overview of the Category

2.1 Definition

Critical Vulnerabilities & Patch Management incidents occur when high- or critical-severity software flaws exist and are being exploited (or at imminent risk) — including zero-days (no vendor patch available) and high-impact CVEs with active exploitation. Effective response requires rapid detection, compensating controls, and coordinated patching or mitigation.

2.2 Common Attack Chain

1. **Discovery / Disclosure:** vendor bulletin, exploit PoC, or threat intel indicating active use (zero-day / disclosed CVE).
2. **Reconnaissance by attacker:** scanning for vulnerable versions, targeted probing.
3. **Exploit:** remote code execution, privilege escalation, or bypass leading to foothold.
4. **Post-Exploit Activities:** lateral movement, persistence, data theft or further payload deployment.
5. **Mitigation / Patch:** vendor patch, configuration change, or compensating control deployment; verification and remediation.

2.3 Primary Risks & Business Impact

- Rapid, widespread compromise of critical infrastructure (DCs, production workloads).
- Data breach, service disruption, and high remediation cost.
- Reputational damage and regulatory exposure for delayed response.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	MTTD Goal	MTTR Target

Critical	Zero-day in widely-deployed software with confirmed in-the-wild exploitation or PoC and accessible attack surface.	$\leq$ 15 min	Contain mitigations within 4 hrs; full remediation/patch rollout depending on vendor (24–72 hrs for workarounds; patch window as vendor releases).
High	Public CVE with proof-of-concept and scanning activity; exploitation observed in limited scope.	$\leq$ 1 hr	Emergency patch/mitigation within 24–72 hrs.
Medium	Vulnerability reported but no active exploitation; targeted systems only.	$\leq$ 24 hrs	Scheduled patch during next maintenance window (3–14 days).
Low	Non-critical or low-impact vulnerability; routine patching.	$\leq$ 30 days	Regular patch cycle (30–90 days).

Table 1: Severity Matrix - Critical Vulnerabilities & Patch Management

4 Tools & Preparation (Recommended)

- **Vulnerability Management:** Qualys, Tenable, Rapid7 — centralised discovery, asset prioritization, and CVSS-based scoring augmented with business context.
- **Patch Orchestration:** SCCM/WSUS, Ansible, Puppet, Jamf, cloud-native patch services.
- **Telemetry & Detection:** EDR (process creation, suspicious modules), SIEM (aggregation of vuln scans, IDS alerts), network IDS/IPS, web application protection, and host integrity monitoring.
- **Threat Intel:** vendor advisories, CERT/ICS-CERT, CISA KEV, vendor contact lists, and commercial intel feeds.
- **Change Management / CAB:** pre-authorized emergency change procedures, rollback plans, and validation testbeds.
- **Forensics / IR Tools:** memory imaging tools, disk forensics, network packet capture, and offline test environments for safe patch testing.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- Vendor bulletin / CISA/mitigation guidance indicating zero-day or active exploitation.

- EDR alerts for exploit-specific behavior (unexpected DLL injection, suspicious child processes).
- SIEM correlation: sudden scanning for specific endpoint versions or targeted PoC patterns.
- IDS/IPS signature hits and honeytoken triggers for known exploit patterns.

Quick actions:

- Confirm authenticity of advisory, map affected asset inventory, and classify severity using the matrix.
- Convene emergency Vulnerability Response Team (VRT) including IT Ops, change control, application owners, legal and communications.
- Capture detection artifacts (packets, logs, memory images) from suspected exploited hosts.

5.2 Containment (Immediate / Short-term)

- Apply compensating controls where patch not yet available: network segmentation, WAF rules, access-control restrictions, disable affected services, or apply vendor-recommended mitigations.
- Block scanning/exploit IPs at perimeter and deploy IDS/IPS signatures for the exploit.
- Isolate confirmed compromised systems for forensic capture and prevent lateral movement.

5.3 Investigation & Forensic Triage

- Collect full timeline: patch levels, recent changes, account activity, process trees and memory images.
- Determine scope of compromise (which assets accessed, persistence mechanisms used, data accessed/exfiltrated).
- Test vendor patches/mitigations in staging to validate rollback strategies and compatibility.

5.4 Eradication

- Remove exploited artifacts, rotate credentials, and reimage hosts as required.
- Apply vendor patches or in-house hotfixes; if vendor patch unavailable, apply robust mitigations (e.g., disable vulnerable feature, firewall rules).
- Validate remediation with secondary scans and targeted tests (full regression and acceptance tests).

5.5 Recovery

- Reintroduce systems to production in a phased manner with enhanced monitoring.
- Continue intensive monitoring for at least 30–90 days for signs of re-exploitation or persistence.
- Reassess SLAs and business continuity impacts; restore services from validated backups if integrity suspect.

5.6 Post-Incident Activities

- Full incident report including timeline, affected assets, IOCs, root cause, and remediation actions.
- Update patch management policies, emergency CAB procedures, and asset inventory/CMDB hygiene.
- Conduct lessons-learned, tabletop exercises simulating zero-day scenarios, and update playbooks.

6 MITRE ATT&CK Framework Mapping

Critical Vulnerabilities & Patch Management - ATT&CK Mapping

- **Initial Access / Exploitation:** T1190 (Exploit Public-Facing Application), T1203 (Exploitation for Client Execution)
- **Persistence / Privilege Escalation:** T1547 (Boot or Logon Autostart Execution), T1068 (Exploitation for Privilege Escalation)
- **Discovery / Lateral Movement:** T1087 (Account Discovery), T1021 (Remote Services)
- **Impact / Exfiltration:** T1486 (Data Encrypted for Impact), T1041 (Exfil over C2)

7 Key Telemetry & Logs to Collect

- EDR process creation, module loads, and command-line logging; Sysmon process/image load and network events.
- SIEM correlation of vuln-scanner results, IDS/IPS alerts, and vendor advisory indicators.
- Network PCAPs for exploit attempts, application logs for abnormal input patterns, and authentication logs for suspicious access.
- Patch management system logs (who applied what and when), CMDB asset versions, and container image SBOMs.

8 Subcategory Scenarios (Realistic)

Note: Scenarios are operational SOC/IR narratives — detection, investigation, containment, eradication, recovery and lessons learned.

Scenario A: Zero-Day Exploit Detection — RCE in Widely-Used Web Proxy

Summary: A vendor advisory (and subsequent threat intel) reports a zero-day remote code execution (RCE) in a widely-deployed reverse-proxy used by the organization. PoC is circulating. EDR telemetry shows suspicious processes spawned from the proxy service on a DMZ host.

Detection:

- Threat intel / vendor bulletin: zero-day with PoC details and indicators.

- EDR: unexpected child process (shell) spawned by proxy process and outbound connection attempts to unknown hosts.
- IDS: exploit-style payload observed in HTTP traffic matching PoC patterns.

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* due to zero-day and confirmed exploit attempts. Emergency VRT called.
2. **Immediate containment:** Place proxy instances behind stricter ACLs, redirect public traffic to temporary CDN/WAF frontends, and apply vendor-recommended mitigations (disable vulnerable module) if available.
3. **Forensic collection:** Isolate affected hosts, collect memory images, web logs, PCAPs and the running process tree; snapshot container images.
4. **Hunt:** Search estate for other proxy instances with same version and for similar EDR or IDS indicators.

Containment & Eradication:

- Apply in-place mitigations (WAF rules to block exploit URI patterns, disable features) and block hostile IPs.
- If vendor patch available: test in staging, then perform emergency rollout with rollback plan. If no patch: enforce isolation and compensate via network controls and traffic filtering.
- Reimage compromised hosts where arbitrary code execution occurred.

Recovery:

- After patches/mitigations, gradually reintroduce services behind hardened controls and monitor closely for suspicious reactivity.
- Rotate any credentials or tokens present on compromised hosts and verify integrity of backup images.

Outcome & Lessons:

- Improve asset inventory and automated detection of vulnerable versions; pre-approve emergency patching workflow to reduce time-to-patch.
- Maintain WAF rule templates and capability to rapidly redirect traffic to protected frontends.

Scenario B: Exploit in the Wild — Vulnerability in Database Engine with Patch Available but Not Yet Deployed

Summary: A high-severity CVE in a popular database engine has an available patch. Attackers begin scanning for vulnerable versions and evidence shows limited exploitation attempts against a staging environment that was not patched.

Detection:

- Vulnerability feed: published CVE with vendor patch.
- SIEM: scanning activity for database port and IDS signatures for exploitation attempts.

- Application logs: anomalous SQL statements and failed authentication attempts on staging DB.

Investigation & Actions:

1. **Triage & classification:** Classified as *High*. Patch available but not in all environments.
2. **Immediate containment:** Isolate staging DB from internet access, block scanning sources, and restrict DB access to trusted networks.
3. **Forensic collection:** Preserve DB logs, audit trails, and copies of suspicious queries; inventory all DB instances and patch status.

Containment & Eradication:

- Perform emergency patch deployment on staging and plan controlled rollout to production with pre-deployment tests; apply DB-level access controls and temporary IP allowlists.
- Rotate DB credentials and service accounts associated with the affected instances.

Recovery:

- Validate patched systems and restore any altered data from verified backups if tampering discovered.
- Update patch baseline and enforce faster patch cadence for critical CVEs.

Outcome & Lessons:

- Improve automated patch deployment and tracking; reduce drift between staging and production patch levels; enforce standard maintenance windows with emergency exception handling.

Scenario C: Patch Management Failure — Incompatible Patch Causes Outage and Provides Attack Window

Summary: An emergency patch rollout for a critical agent caused service instability on several hosts. During the outage window, attacker scanned and exploited an unpatched subset that had been excluded from the patch batch due to compatibility concerns.

Detection:

- Change-control logs: emergency patch applied; multiple hosts failed and were rolled back.
- Monitoring: service errors and degraded performance on rolled-back hosts.
- IDS: scanning activity increases targeting rolled-back hosts.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to exposure during patch rollback window.
2. **Immediate containment:** Isolate rolled-back hosts, apply temporary compensating controls (network ACLs, WAF rules), and restrict admin access.
3. **Forensic collection:** Collect change logs, rollback details, host logs and any suspicious access attempts during the window.

Containment & Eradication:

- Coordinate with vendor/engineering to produce a tested patch variant; use staged rollouts and canary hosts to validate before mass deployment.
- Where immediate patching impossible, apply strict network segmentation and virtual patching (IDS/WAF signatures).

Recovery:

- Once compatible patch verified, perform controlled re-deployment, validate host stability and lift emergency ACLs carefully.
- Review rollback procedures and improve pre-deployment testing to avoid future exposure windows.

Outcome & Lessons:

- Strengthen pre-deployment compatibility testing, maintain a canary pool, and formalize a "virtual patch first" policy (WAF/IDS rules) while vendor fixes are validated.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Detect exploit-like HTTP payloads (example Splunk):

```
index=web sourcetype=access_combined
| search request_uri="*exploit_string_or_pattern*"
| table _time host clientip request_uri useragent
```

Inventory unpatched hosts (example):

```
vuln_scan_results
| where CVE == "CVE-XXXX-YYYY" and PatchStatus == "Missing"
| table host,ip,os,package_version
```

9.2 Appendix B — Patch Emergency Checklist (Quick Reference)

- Verify advisory authenticity (vendor, CISA, CERT).
- Map affected asset inventory (CMDB/SCCM).
- Convene emergency VRT CAB (pre-authorized emergency change if required).
- Apply mitigations (network controls, WAF, disable feature) if patch unavailable.
- Test patch in staging (canary), document rollback plan, and schedule emergency rollout.
- Collect forensic evidence if exploitation suspected before remediation.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Severity / Playbook invoked.
- Affected assets, CVE(s), vendor advisory references, and exploit indicators (IOCs).
- Actions taken (mitigations, patches, reimages) with timestamps and owners.
- Evidence preserved (PCAPs, memory images, logs) and follow-up items (patch compliance, process changes).
- Communications performed (internal/external) and regulatory considerations.