CAPTAIN Cyberscaler

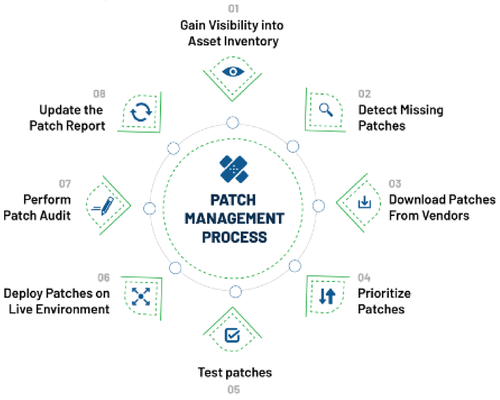
CAPTAIN CYBERSCALER VULNERABILITY AND PATCH MANAGEMENT

→ RECORD 28,961 VULNERABILITIES DISCLOSED IN 2023!

- Over 7,000 vulnerabilities had proof-of-concept exploit code.
- 206 had weaponized exploit code available, highly likely to compromise the target system.
- About 50 were zero-day exploits, targeted for exploitation on the same day of disclosure.
- 97 vulnerabilities were exploited in the wild but not included in the CISA KEV (Known Exploited Vulnerabilities) list.

→ SUMMARY OF SERVICES

Patch Management Process Flow



1. IDENTIFICATION AND PRIORITIZATION OF PATCHES

2. DEPLOYMENT OF PATCHES

- Pending patches
- Failed patches
- Missing patches
- Schedule patching

3. MONITORING AND VERIFICATION

- Ensure patches are successfully applied and functioning as intended.

→ General Operation

- Patch Management
  - o Identifying, acquiring, installing, and verifying patches to address vulnerabilities, bugs, or enhance functionality.
  - o Verifying patches (code changes) for software applications and systems to address vulnerabilities, bugs, or enhance functionality.

- Identification and Prioritization of Patches
- Deployment of pending patches, failed patches, missing patches, and schedule patching.
- Monitoring and verifying that patches have been successfully applied and are functioning as intended.

THANK YOU

CAPTAIN HYPERSCALER, LLC

→ PATCH PROCESS:

- Patch Synchronization: Collect information from vendor sites and synchronize with the product server.
- Patch Detection: Identify devices with missing patches via automatic scans.
- Download: Retrieve missing patches, including security updates, non-security updates, service packs, rollups, optional updates, and feature packs.
- Test and Approve: Test patches in non-production environments to avoid post-deployment issues.
- Deployment: Flexible policies to select deployment windows and create patching policies.
- Report: Generate and customize reports post-deployment, shareable in multiple formats.

→ CLIENT RESPONSIBILITIES

- Work with Captain Cyberscaler to define patching processes, test environments, and scheduling.
- Define maintenance windows for server and application patching and reboots.

→ SERVICE LEVEL AGREEMENT (SLA)

- Emergency Zero-Day Exploits: Immediate patching as soon as patches are available, considering testing and downtime.

→ NON-EMERGENCY PATCHING SLAS:

Score	DMZ Remediation	Data Center Remediation
Critical	< 14 days	< 30 days
High	< 30 days	< 90 days
Medium	< 90 days	< 180 days
Low	< 180 days	Periodically

For more information on how our Vulnerability and Patch Management services can protect your systems, please contact us.

+1 248-395-3989

https://captainhyperscaler.com