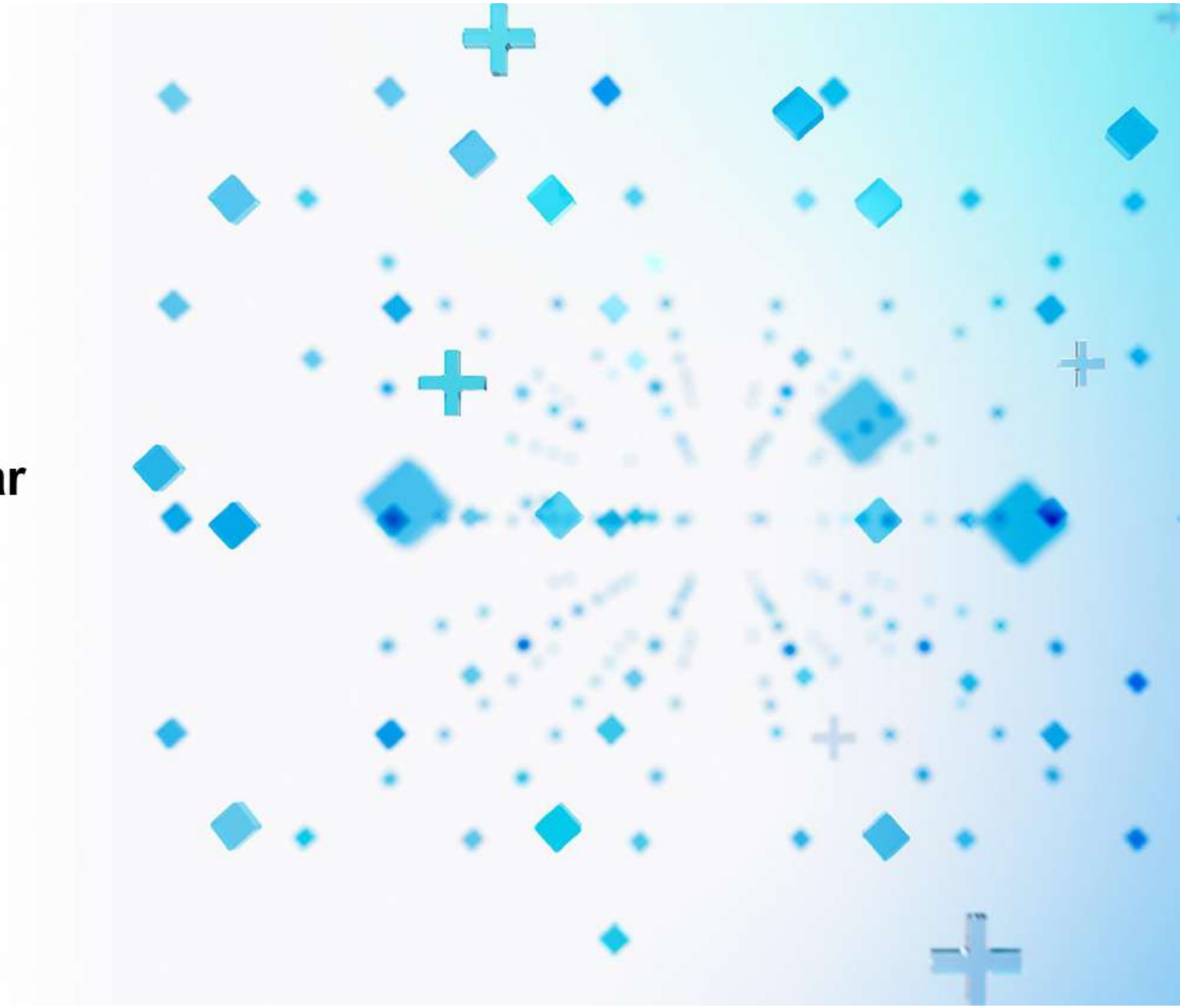
HCLSoftware

HCL BigFix

Patch Tuesday Webinar

October 2026



Agenda

01 Month at a glance - The beatings will continue until morale improves

02 Vulnerability breakdown by type

03 A scoring system primer

04 Vulnerability deep dive

Month at a Glance

1,422
Total CVEs

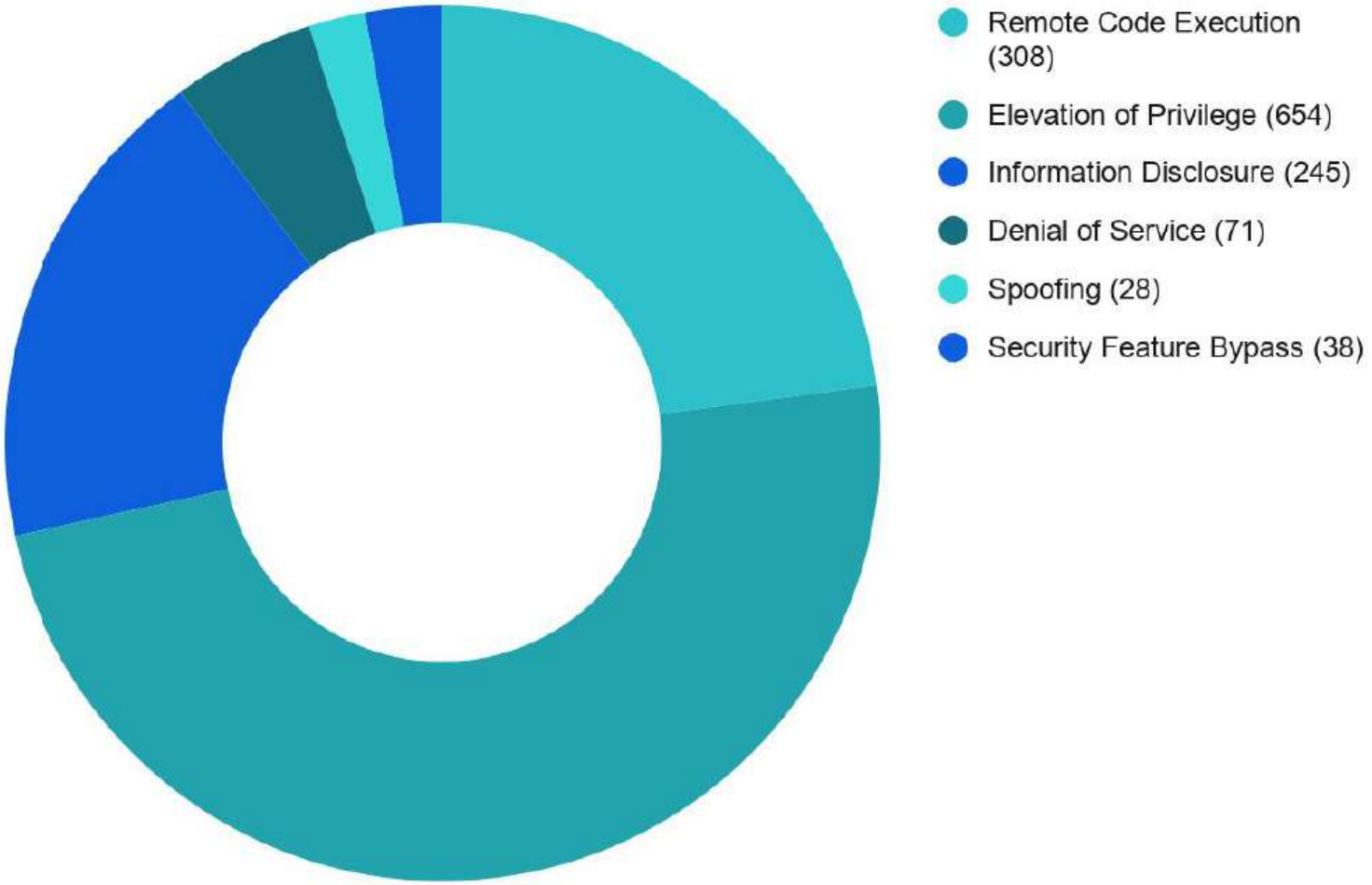
2
Zero-Day Threats

Acceleration Recommended For:

- Failover Clusters
- DNS Servers & DHCP Servers
- Domain Controllers
- Wireless Authentication Servers
- Web Servers
- Print Servers



This Month's Vulnerability Breakdown by Type



SECURITY PERSPECTIVE

Prioritizing Vulnerabilities

A winding journey through how my brain evaluates vulnerabilities

- Deconstructing the flaws in CVSS, EPSS, KEV
- Balancing patching urgency vs. operational risk
- Contextual exposure over raw vulnerability scores



CVSS - Common Vulnerability Scoring System

How Does the Exploit Work?

A mechanical view lacking context and high-resolution fidelity.

1. Low Granularity - only a few values to pick from in each category, relies on the judgment of the reporter

2. Attack Vector: Network lumps all these into one value:

- Incoming connections
- outgoing connections
- Files delivered over network

3. Distorts severity

Files that then have to be clicked on are nowhere near the real severity of an incoming network attack.

EPSS - Exploit Prediction Scoring System

How likely is this to be exploited in the next 30 days?

- Makes no judgment on the severity of the impact
- Does not consider value of the target component
- Overweights vulnerabilities with file-delivery mechanisms
- Data generated via machine learning
- Gets more accurate each day after a CVE is published

CISA KEV with BOD 26-04

- **How soon do you need to fix this vulnerability?**



- Limited binary categorization
  - Internet exposure
  - Fully automatable
  - Known Exploited Vulnerability
  - Full or partial control

- Only three states - 3 day, 14 day, or 60 day remediation window

JVSS - Joe Vulnerability Scoring System



THREAT ACTOR ROI

If I were a business, which vulnerability would I go after first?

(Threat groups ARE a business!)

ATTACKER CONNECTIVITY

How does an attacker connect to the affected component?

Evaluates specific exposure paths:

- **Internet Exposure**
- **Intranet Access**
- **Subnet Isolation**

DEFENSIVE BYPASS

Does it circumvent regular defensive behaviors?

Factors in complexity controls like sandbox escapes and the required number of clicks to successfully exploit.

JVSS - Joe Vulnerability Scoring System ™

Key evaluation questions for assessing vulnerability reachability, environment, and impact

Exploit Impact

What are the implications of an exploit?

Threat Chaining

Does it interact with any other current exploits?

Default State

Is this installed by default?

Network Exposure

How available is the service from various networks?



HCLSoftware

Four systems, four different questions

What each signal contributes, and where its view narrows

CVSS

SEVERITY ESTIMATE

How does the exploit work?

CONTEXT LIMIT

A few metric values can collapse different routes into "Network": inbound access, outbound connections, or a file that needs a click. No application-specific context.

EPSS

EXPLOIT FORECAST

How soon might exploitation happen?

CONTEXT LIMIT

Estimates observed exploitation within 30 days, not impact or target value. File-delivery vulnerabilities may rise too high. Scores evolve as signals accumulate after disclosure.

KEV + BOD 26-04

REMEDIATION WINDOW

How soon must it be fixed?

LIMITED CATEGORIES

Public exposure, KEV status, exploit automation, and partial or full control map to three windows: 3, 14, or 60 days.

JVSS

BUSINESS PRIORITY

Which would an attacker exploit first?

JOE'S ANALYSIS

Map real reachability: internet, intranet, or subnet. Weigh defensive bypass, exploit impact, and interaction with current exploits.

JVSS adds the paths, defenses, and consequences that generic signals cannot see.

HCLSoftware

Excluded 9.8 Severity Items

Components That Didn’t Make The List This Month

- Windows Error Reporting ×3
- Windows Text Shaping ×3
- Windows Command Shell
- Windows Volume Manager
- CCFFilter Driver
- Windows Media Player
- Windows OLE Driver
- Microsoft Office
- Microsoft Outlook ×5
- OpenSSH



HCLSoftware

Criticals

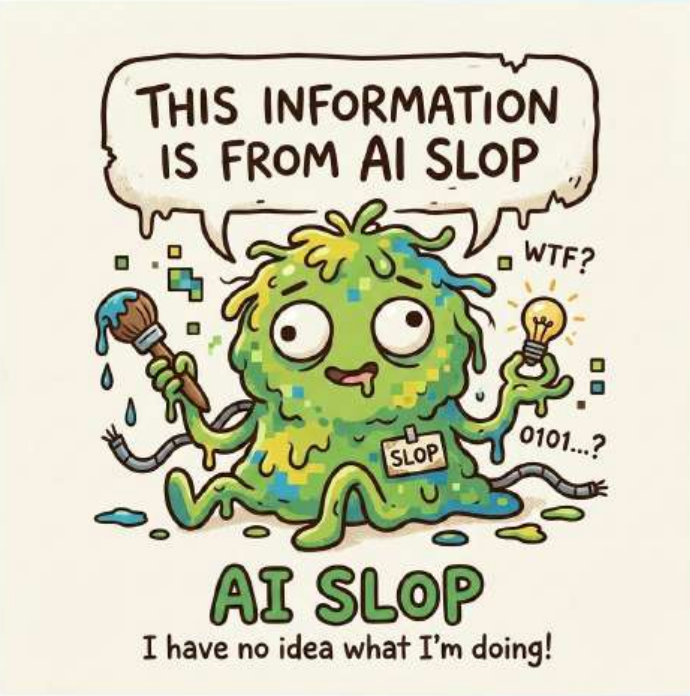
CVE-2026-105010 – 9.8

Windows Search elevation of privilege

Conflicting information abound!

- Description= RCE
- Title and Summary = elevation of privilege.

Summary says “send a malicious packet”, but the service doesn’t listen on any ports!



Zero days

CVE-2026-96951 • CVSS 8.8

ACTIVE EXPLOIT

Windows Shell mark of the web bypass

Maliciously crafted files can skip mark of the web dialogs.

CVE-2026-108398 • CVSS 8.8

ZERO DAY VULNERABILITY

Windows Defender Application control bypass

Skip application execution rules locally.

Criticals

CVE-2026-83910 • CVE-2026-96219 • CVE-2026-97805

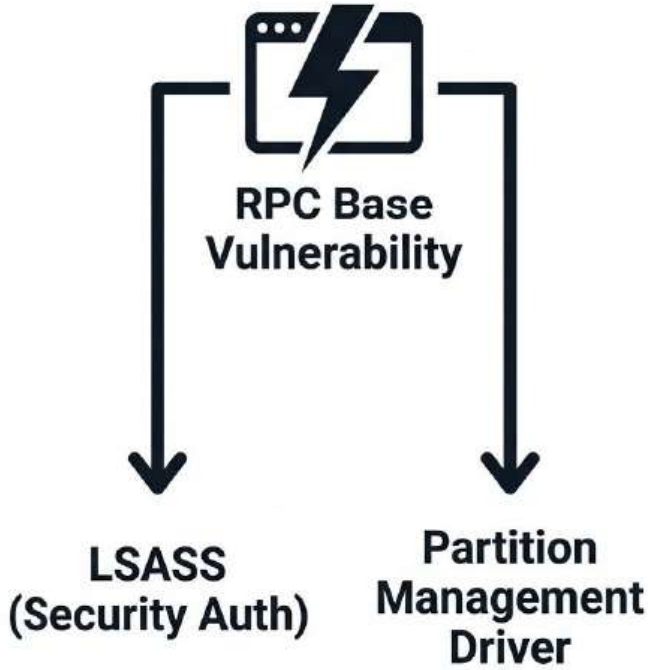
CVSS Score: 9.8 Critical

Remote Procedure Call (RPC) Root RCE

! Installed by default on all Windows boxes.

Impact Scope:

Subcomponents **Local Security Authentication Sub System (LSASS)** and **Partition Management driver** are directly affected via the underlying RPC vulnerability.



Criticals: Web Server Vulnerabilities

CVE-2026-70024 – 9.8

IIS RCE

Internet Information Services

IIS servers vulnerable to a single packet takeover.



CVE-2026-70188 – 9.1
CVE-2026-88092 – 9.1

ASP.Net Bypass

Security Feature Bypass

- Malicious HTTP/2 requests can bypass authentication on web servers and impersonate any user.
- HTTP/1.1 requests can inject commands to the server.

CVE-2026-105016 – 9.8
CVE-2026-100219 – 9.8

MS QUIC RCE

Multiple Single Packet RCEs

- Most web servers use MS QUIC to serve multiple streams at once to a browser.
- Multiple single packet RCE CVEs exposing web server instances to immediate remote takeover.

Criticals

COMMON THREAD: INFRASTRUCTURE SERVER VULNERABILITIES

DNS Server RCE

CVE-2026-83869

CVSS Score: 9.8

Malicious requests against a DNS server can achieve remote code execution.

DHCP Server RCE

CVE-2026-96320 / CVE-2026-96934

CVSS Score: 9.8

DHCP servers configured in failover mode can have their memory corrupted by a malicious request, enabling RCE or a service crash.

Kerberos Auth Bypass

CVE-2026-85844

CVSS Score: 9.8

An attacker can bypass Kerberos authentication and achieve SYSTEM privileges on a domain controller.

Criticals

CVE-2026-70147 – 9.8

CVE-2026-70153 – 9.8

Print server RCE

Malicious print jobs can PC LOAD LETTER your whole infrastructure



Criticals

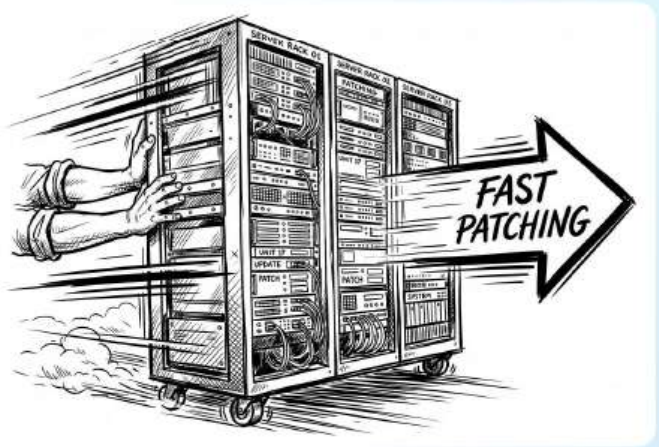
CVE-2026-102192 – 7.5

CVE-2026-96864 – 9.8

Windows Failover Cluster Denial Of Service and RCE

Multiple vulnerabilities in the Failover cluster allow Remote Code Execution (RCE).

Many companies patch clusters manually and delay patch application. **Consider pushing these forward this month.**



Criticals

CVE-2026-100222 – 9.8

CVE-2026-85806 – 9.8

Network Policy Server RCE



Low complexity network RCE against your wireless network authentication controller. Extra threatening due to wireless access.

Exists running service “IAS”