HCLSoftware

HCL BigFix

Patch Tuesday Webinar

August 2026

Agenda

01 Month at a glance - slightly less of a flood

02 Vulnerability breakdown by type

03 DNS servers under assault

04 Automation - how early is too early?

05 BigFix MCP server release

Microsoft CVE’s at a Glance in August 2026

Total CVEs

422

Active vulnerabilities tracked and addressed across systems this month.

Critical Threats

3

Zero-day exploits discovered requiring urgent remediation actions.

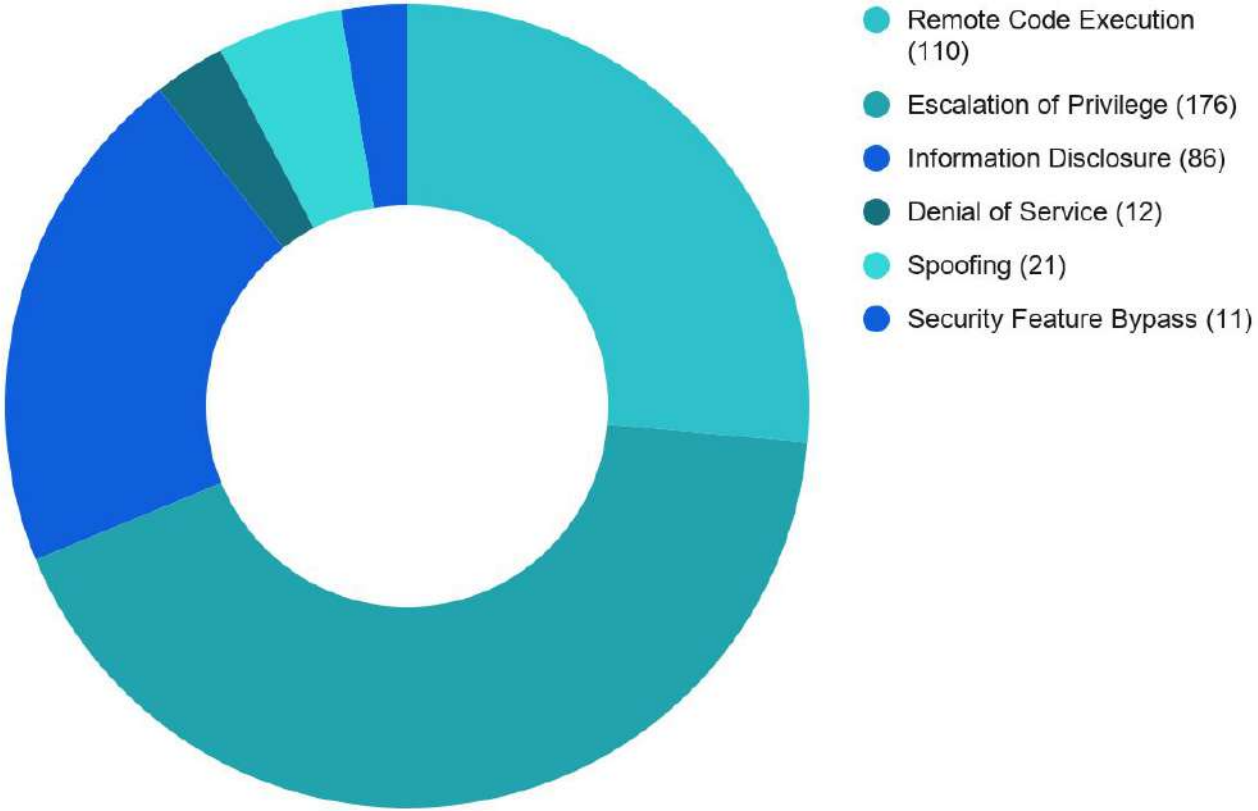
Acceleration Focus

Targeted prioritization deployed for key infrastructure:

- **DNS Servers**
- **Web Servers**
- **Many optional server roles**
- **SharePoint**
- **MSMQ**

HCLSoftware

This Month’s Vulnerability Breakdown by Type



All Local Zero Days

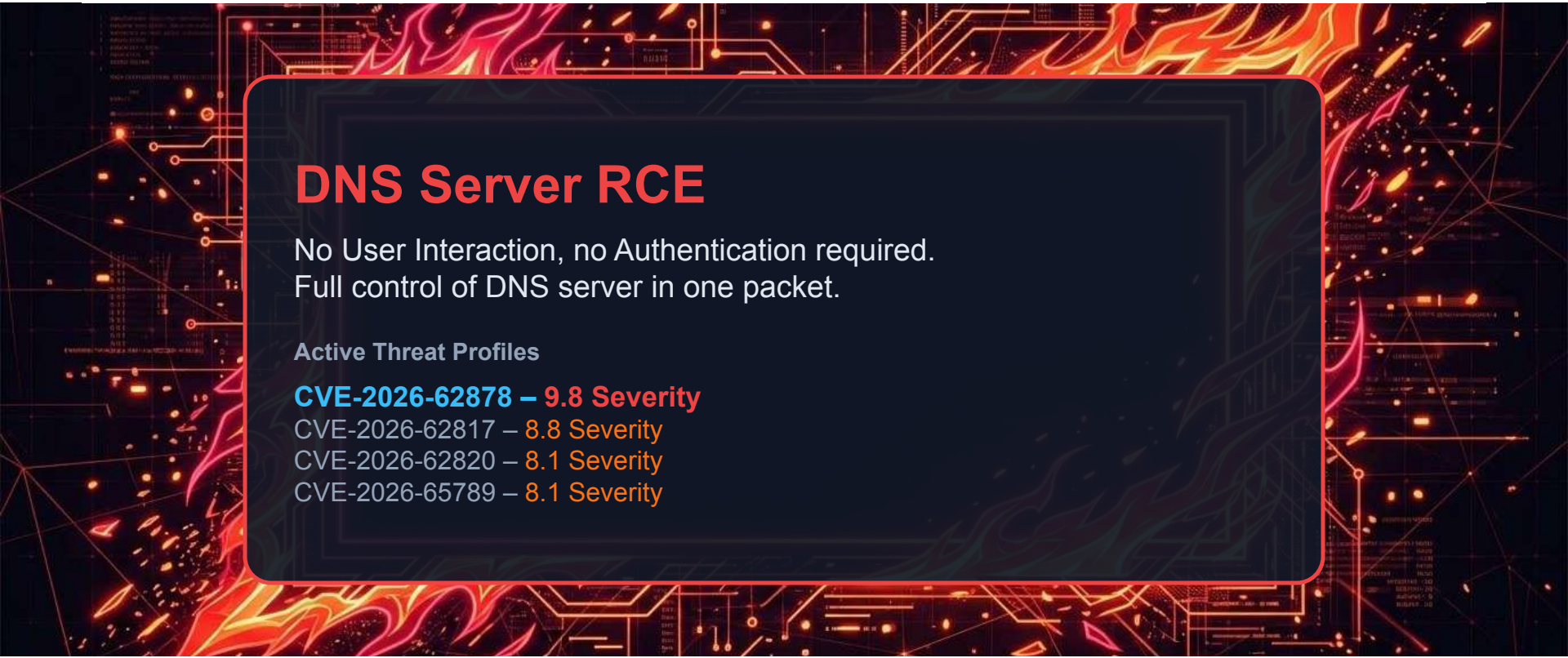
Refreshingly low priority

CVE-2026-68820 — 7.0 (Winsock EOP)
Local elevation of privilege attack

CVE-2026-62832 — 7.8 (User Profile EOP)
Local elevation of privilege attack

CVE-2026-72971 — 5.5 (Container Filter)
Local data tampering vulnerability

Extra Critical



DNS Server RCE

No User Interaction, no Authentication required.
Full control of DNS server in one packet.

Active Threat Profiles

CVE-2026-62878 – 9.8 Severity
CVE-2026-62817 – 8.8 Severity
CVE-2026-62820 – 8.1 Severity
CVE-2026-65789 – 8.1 Severity

SharePoint Attack Chain in Two Clicks

CVE-2026-65660 (STEP 1)

6.5 CVSS Score

SharePoint Spoofing Vulnerability

An authenticated user can impersonate any other user in the environment.

CVE-2026-65663 (STEP 2)

8.8 CVSS Score

SharePoint Remote Code Execution

A Site Owner can execute arbitrary code in the context of the server service.

Criticals

CVE-2026-62815

9.8 CVSS Score

Microsoft QUIC Remote Code Execution

QUIC - Quick UDP Internet Connections

No UI and no Auth required attack against web servers like IIS and SMB.

HCLSoftware

Criticals

CVE-2026-62819

8.1 CVSS Score

Routing and Remote Access Service RCE

RRAS service allows a Windows server to act as a router. External IP address is vulnerable to no auth and no UI remote code execution.

BigFix Relevance

```
exists running service "RemoteAccess"
```

Criticals

CVE-2026-62893

9.8 CVSS Score

Windows Deployment Services TFTP Server RCE

No UI and no authentication required.

Vulnerability in the PXE hosting systems allows an attacker to run code as the WDS server.

HCLSoftware

Criticals

CVE-2026-62889

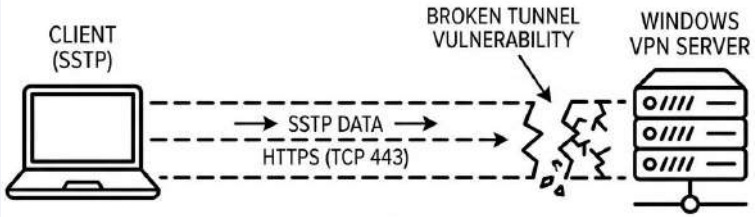
8.1 CVSS Score

Windows Secure Socket Tunneling Protocol RCE

No UI and no authentication required.

SSTP is the built-in Windows VPN service.

exists running service "SstpSvc"



SECURE SOCKET TUNNELING PROTOCOL (SSTP) - VULNERABILITY DIAGRAM

Criticals

CVE-2026-65791

9.8 CVSS Score

Windows iSCSI Target Service RCE

No UI and no authentication required.

Optional iSCSI remote storage service is vulnerable to single packet RCE.

BIGFIX DETECTION

Relevance Language

Verify if the system is vulnerable by checking for the active running service:

```
exists running service "msiscsi"
```

Criticals

CVE-2026-62823

8.1 CVSS Score

DHCP Server RCE

DHCP servers vulnerable to single packet attack from an adjacent network.

Criticals

CVE-2026-62816

8.8 CVSS Score

Reliable Multicast Transport Driver RCE

No UI and no authentication required.

RMCAST powers the Microsoft Message Queueing service.

BIGFIX DETECTION

Relevance Language

Verify if the system is vulnerable by checking for the active running service:

```
exists running service "msmq"
```

Criticals

CVE-2026-59124

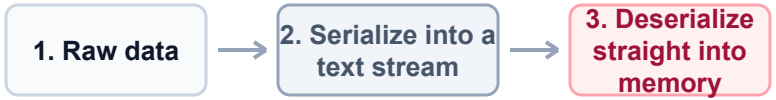
9.8 CVSS Score

High Performance Computing RCE

HPC does not verify payloads before deserializing requests into in-memory objects.

Allows an attacker to run arbitrary code with no authentication.

Note: Listed as a Windows App Client vuln??



⚠️ **No Verification Step**

Because HPC immediately deserializes incoming streams without validating the payload, an attacker can instantiate arbitrary execution trees.

💥 **Result: Unauthenticated Remote Code Execution**

Volume and Quality of Vulnerability Discovery

AI Research

AI Research has significantly increased the volume of vulnerabilities for Vendors and Customers to manage, respond to, and report.

AI Slop

AI Slop has introduced a significant amount of background noise into the landscape, heavily complicating verification and triage workflows.

Everybody Wants More Automation

The Vision

“We want to get to the point where vulnerability management runs itself”

Technical Capability

Technical ability to automate is already available in BigFix. The core tools and platforms aren't the issue.

The Real Gap

Even without AI slop, some of the effort still requires human decision making right now and will require that until your organization can account for and trust all your decision making to AI.

Hidden Assumptions in the Vulnerability Cycle

Assumption 1

“We’re on a 5/15/30 day cycle, so as long as [vuln] gets patched within that [n] days cycle: it’s fine.”

Reality: Doesn’t account for outliers. What about out of bands? And what about failures for disk space? What about offline systems?

Assumption 2

“CVSS, EPSS, KEV, etc.. risk measurement doesn’t matter; we just patch everything”

Reality: True for the majority of vulnerabilities *assuming the business has a good handle on risk and definition of done.*

Avoid Further Automation Until You've Mastered These

BigFix, if your organization licensed the right entitlements for your needs, enables you to automate vulnerability management***
However, **automation will introduce more problems** if your team is:

Risk Calculation

Unclear on how your organization calculates risk or risk calculation doesn't account for all use cases

Definition of Done

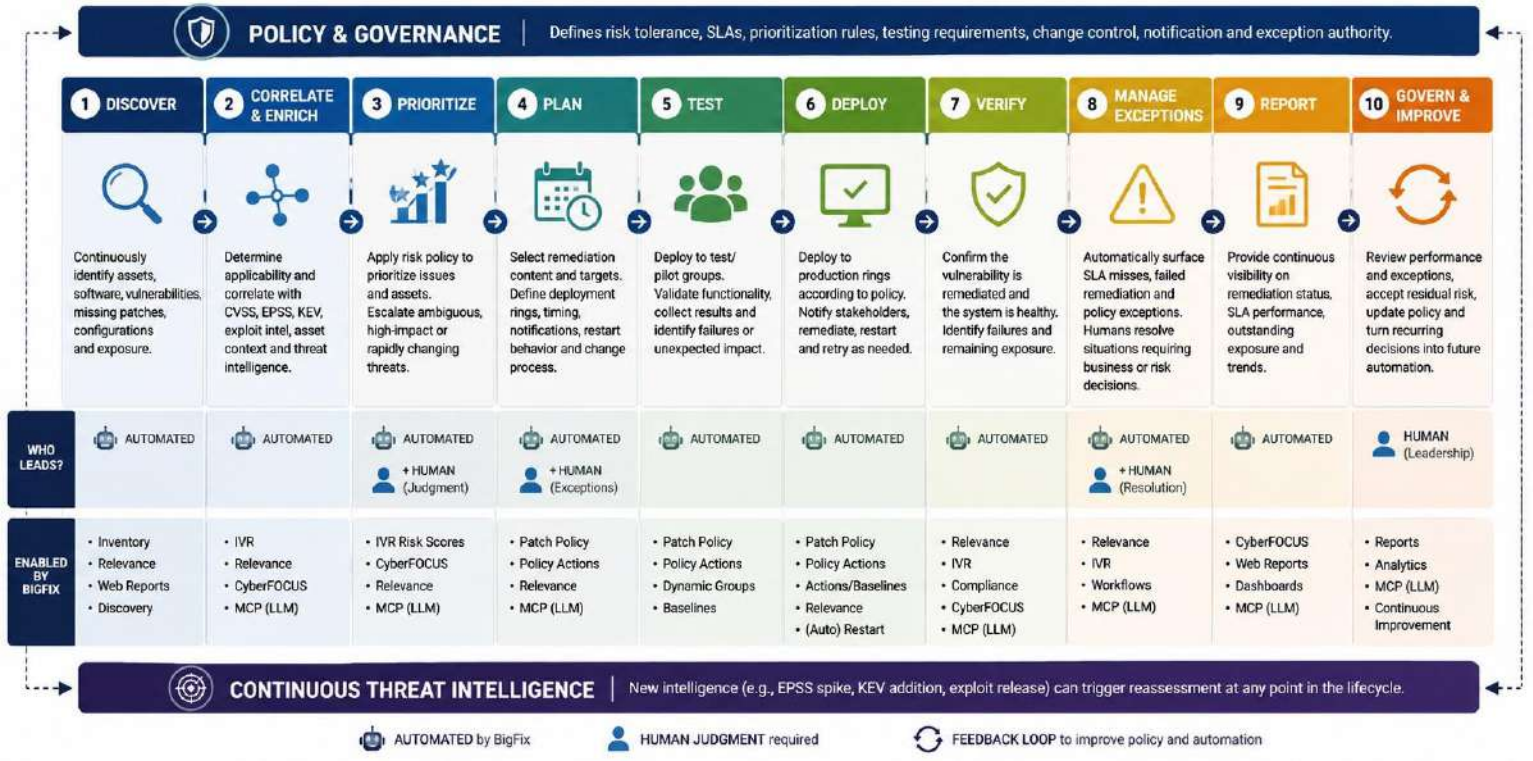
Unclear on your organization's definition of done - deploying a patch doesn't mean the vulnerability is remediated. How big is your backlog?

Outliers & Failures

Not capable of handling outliers or failures within the PLA cycle

THE FULL VULNERABILITY MANAGEMENT LIFECYCLE

Automate the routine. Escalate the exceptional. Improve continuously.



HCLSoftware

New Capability Unlocked: BigFix MCP

Use Your Own AI

Connect BigFix to the LLM your organization already uses and governs. No separate BigFix AI environment is required.

Secure Environment

Works with your LLM and BigFix deployment. Operational data does not need to be shared with BigFix or third-party AI partners.

Go Beyond Q&A

Not just a chatbot. Leverage BigFix APIs to **query, analyze, create, and take action** with customizable controls.

Availability: Offered to all BigFix customers as part of the platform at no additional license cost.

Requirement: BigFix 11.0.6 or higher

HCLSoftware