HCLSoftware

HCL BigFix
Patch Tuesday Webinar

July 2026

Agenda

01 Month at a glance - 3x the vulnerabilities!

02 Vulnerability breakdown by type

03 DHCP servers on the naughty list

04 Mythos ban!

05 Compliance and Inventory releases

Month at a Glance

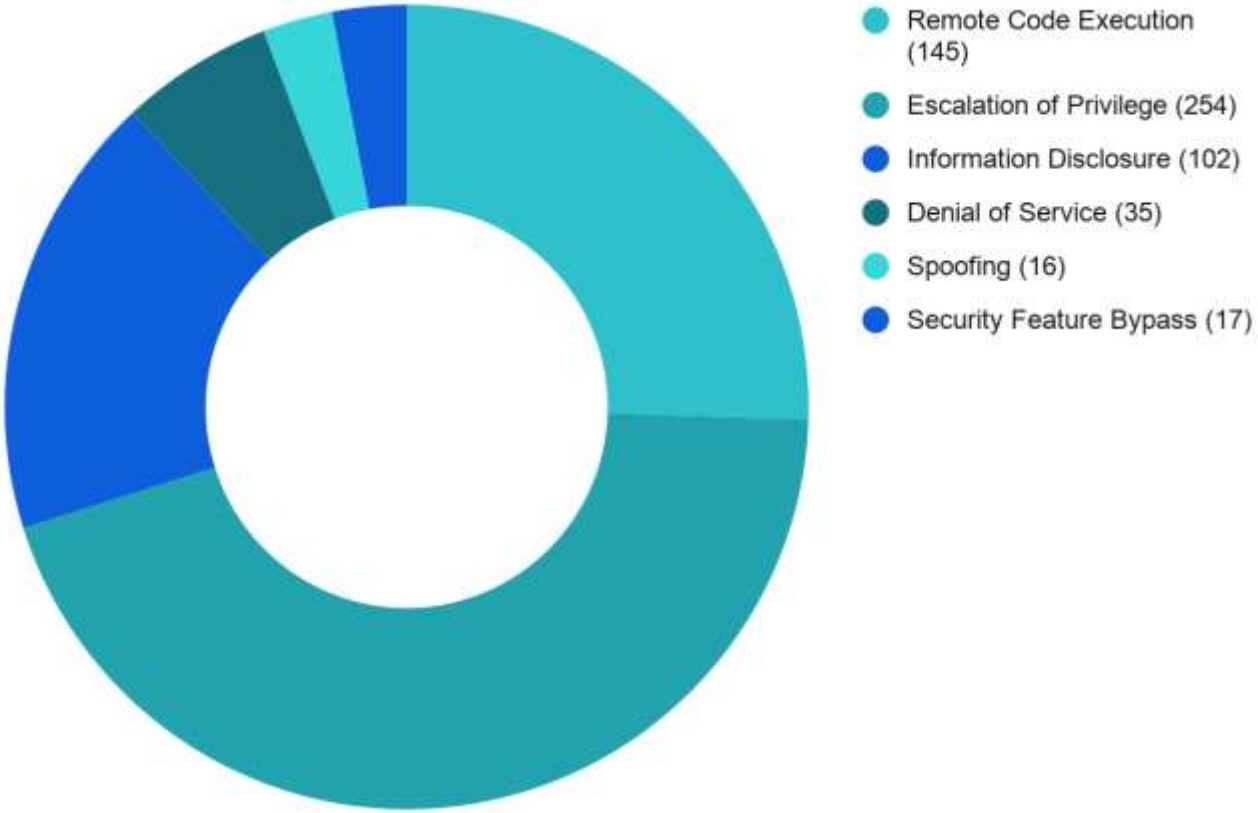
578 CVE’s

3 zero days

Acceleration for:

DHCP servers - FTP Servers - Dynamics - Sharepoint - MSMQ

This Month’s Vulnerability Breakdown by Type



Active Directory Zero day

CVE-2026-49164 – 7.8 **Active Directory Federated Services Zero day Elevation of privilege**

Authenticated user can elevate to Administrator

CVE-2026-49164 – 8.1 **Active Directory Domain Services RCE**

High complexity attack allows control of AD servers

Zero Days

CVE-2026-50661 – 9.1 **Bitlocker Security bypass**

A physical attacker can bypass bitlocker encryption with a USB drive.

If it’s been disclosed for three months, is it a 0 day or a 0 quarter?

Zero Days

CVE-2026-55040 – 9.1

CVE-2026-56164 – 5.3

MS SharePoint Elevation of Privilege

Allows an attacker to bypass all authentication and do whatever they want.

Combine with the next CVE for an extra bad time

Dangerous Criticals

CVE-2026-50522 – 9.8 **MS SharePoint RCE**

Mislabeled score. CVSS=P:N, but the vulnerability requires Site Owner Permissions.

Allows a Site Owner to execute code against the SharePoint server.

Dangerous Criticals

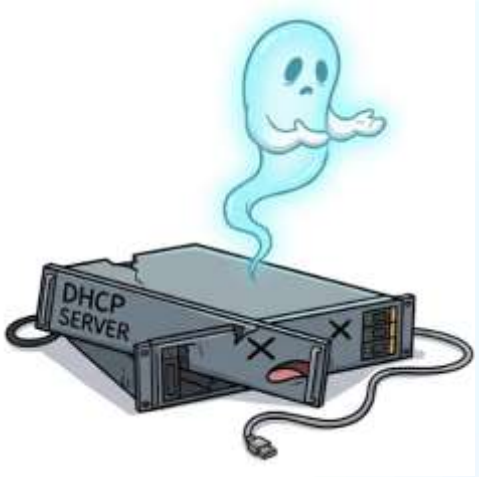
CVE-2026-56159 – 9.8

CVE-2026-50518 – 9.8

CVE-2026-48564 – 8.8

CVE-2026-50370 – 8.8

Windows DHCP Server RCE



No UI, No privileges, network vector.

Instant DHCP server destruction, patch now!

Dangerous Criticals

CVE-2026-49172 – 9.8 **FTP Service RCE**

Any FTP server can be compromised with a single maliciously crafted FTP request.

Exists running service “ftpsvc”

Dangerous Criticals

CVE-2026-54128 – 8.4 **Windows DHCP Client RCE**

A malicious DHCP server can run arbitrary code on a client requesting an IP Address.

Sneaky dangerous for laptops connected to public WiFi

Dangerous Criticals

CVE-2026-50447 – 9.8

CVE-2026-54995 – 8.1

Message Queuing Service and RMCast RCE

Full compromise of any system with a listening MSMQ service.

No user interaction required. Not enabled by default.

Exists running service “msmq”

Criticals

CVE-2026-57092 – 9.9

Hyper-V VMSwitch Elevation of Privilege

Sandbox escape!

Requires a user to run malicious code in a virtual guest. Allows the attacker to run code against the Hyper-V host

Criticals

CVE-2026-55944 – 9.8

Dynamics NAV and Dynamics 365 Business Central RCE

Malicious login attempts can bypass authentication altogether.

Criticals

CVE-2026-56188 – 9.8

Windows Server Network driver RCE

Any windows server can be compromised with a simple race condition from a persistent attacker.

Criticals

CVE-2026-48561 – 9.6 **Copilot for mobile RCE**

A malicious website can cause Copilot for mobile devices to submit and execute prompts without confirmation.

Criticals

CVE-2026-56190 – 9.8 **Remote Desktop Protocol RCE**

If Network Level Authentication is disabled, an attacker can send a packet to a listening RDP device and execute arbitrary code.

Overrated Criticals

CVE-2026-54990 – 9.8

CVE-2026-50474 – 8.8

Remote Desktop Client RCE

CVSS mislabeled again, requires user interaction.

User must connect to a malicious RDP server and manually accept the connection to trigger RCE.

Overrated Criticals

CVE-2026-50380 – 9.6 **GDI+ RCE**

Viewing a malicious EMF+ image file can trigger arbitrary code execution.

Browsers are not an attack vector

Overrated Criticals

CVE-2026-42990 – 9.8

SQL Server ODBC driver elevation of privilege

Dramatically overrated

A client that connects to a malicious SQL server can be compromised. No scope change

Criticals

CVE-2026-55010 – 9.8

Minecraft server RCE?!

Even Steve isn’t safe from Project Glasswing. No auth required RCE against the dedicated server.

Like a whole new kind of exploding Creeper.

Criticals - Standard issue office RCE’s

CVE-2026-50314 – 7.8

CVE-2026-55018 – 7.8

CVE-2026-55022 – 7.8

CVE-2026-55045 – 8.4

CVE-2026-55033 – 7.8

CVE-2026-55127 – 7.8

CVE-2026-55129 – 7.8

CVE-2026-55132 – 7.8

Office preview pane RCE’s

CVE-2026-55056 – 7.8

CVE-2026-55140 – 7.8

CVE-2026-55123 – 7.8

The preview pane beatings will continue until morale improves.

Mythos - drama with the banhammer

- US government shut down all access to mythos/fable on June 12th
- Amazon researchers found ways to break Fable safeguards and receive Mythos security capabilities
- Fable access restored July 1st
- Mythos approval for organizations still ongoing
- https://www.anthropic.com/news/fable-mythos-access

BigFix Inventory 11.0.8 released

- AI Management
  - Discover AI plugins, agents, gateways, and MCP connections.
  - Detailed information on installed AI applications
  - Track AI usage and costs