HCLSoftware

HCL BigFix

Patch Tuesday Webinar

June 2026

Agenda

01 Month at a glance

02 Vulnerability breakdown by type

03 HTTP servers getting roasted

04 Brace yourselves, Mythos is coming

05 Compliance and Inventory releases

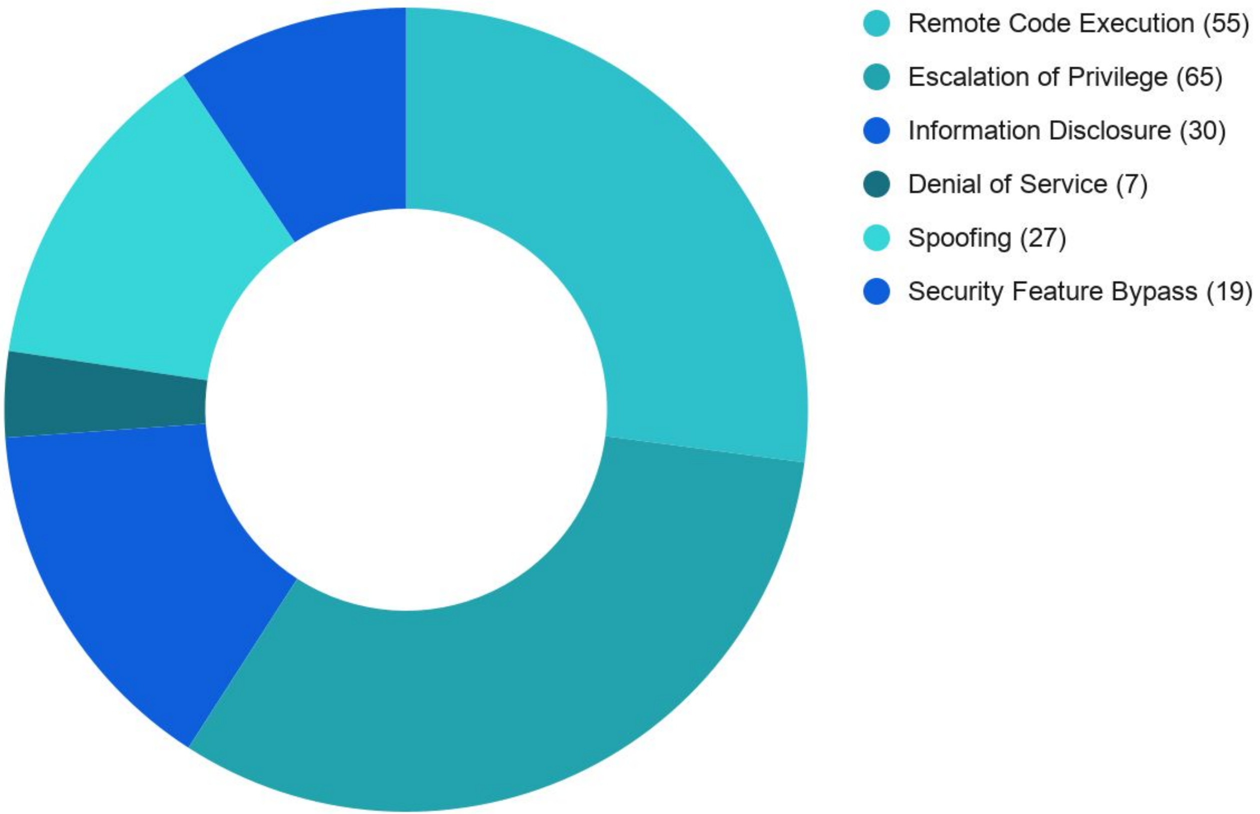
Month at a Glance

200 CVE's

3 zero days

Acceleration for:
DHCP servers - HTTP servers - maybe everything?!

This Month’s Vulnerability Breakdown by Type



Zero Days

CVE-2026-50507 – 6.8 **Bitlocker security bypass**

A physical attacker can bypass bitlocker encryption on a device.

Part of the disgruntled “Nightmare Eclipse” researcher vulnerability drops

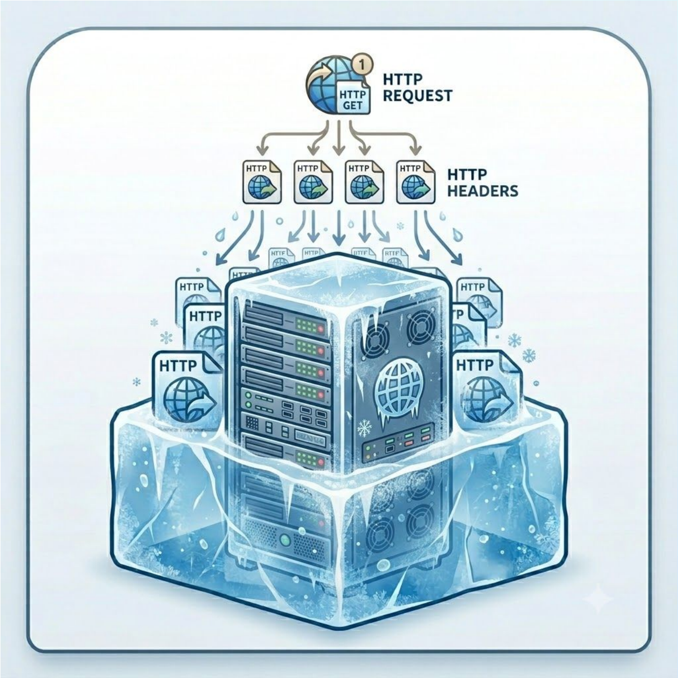
HCLSoftware

Zero Days

CVE-2026-49160 – 7.5 **HTTP.sys Denial of service**

HTTP/2 traffic can contain unlimited amounts of very small headers that consume large amounts of memory.

May freeze or crash HTTP servers.



Zero Days

CVE-2026-45586 – 7.8 **CTFMON Elevation of Privilege**

Local authenticated attackers can elevate to SYSTEM privileges

Criticals

CVE-2026-47291 – 9.8 **HTTP server Remote Code Execution**

Any service relying on http.sys and configured to accept large packets can be used to run arbitrary code. MaxRequestBytes must be < 65535 to be safe.

(exists value "MaxRequestBytes" of it AND (value "**MaxRequestBytes**" of it as integer > **65534**)) of key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters" of native registry

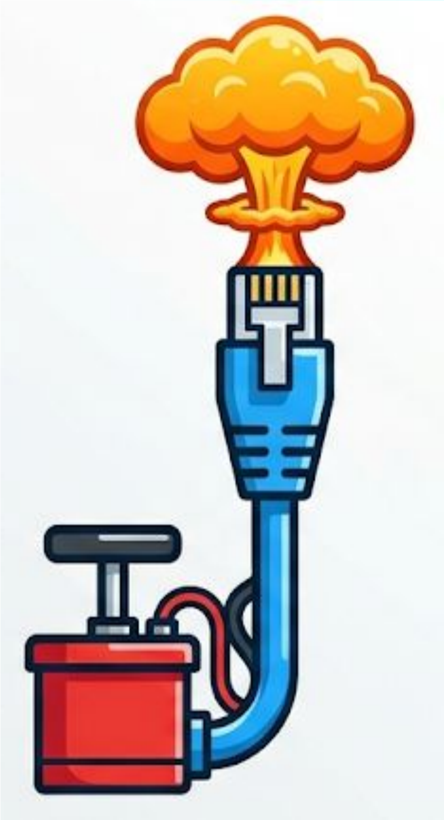
Criticals - IP stack

CVE-2026-45657 – 9.8 **Windows Kernel Remote Code Execution**

TCP/IP vulnerability that allows an attacker to run code as system without any user mistake.

CVE-2026-52904 – 9.6 **TCP/IP Elevation of Privilege**

Local network attackers can elevate to system and execute code with no UI.



Criticals - DHCP servers

CVE-2026-44815 – 9.8 **DHCP Service Remote Code execution**

No UI, no privileges required. Instant takeover of any visible DHCP server.

CVE-2026-45602 – 9.1 **DHCP Tampering Vulnerability**

Possible machine in the middle attack vector. Vulnerability text indicates an attacker can change delivered IP values to clients.

Criticals

CVE-2026-47643 – 9.8

Azure Stack Edge Remote Code Execution

Azure Stack Edge devices can be tricked into creating files or folders in any arbitrary path.

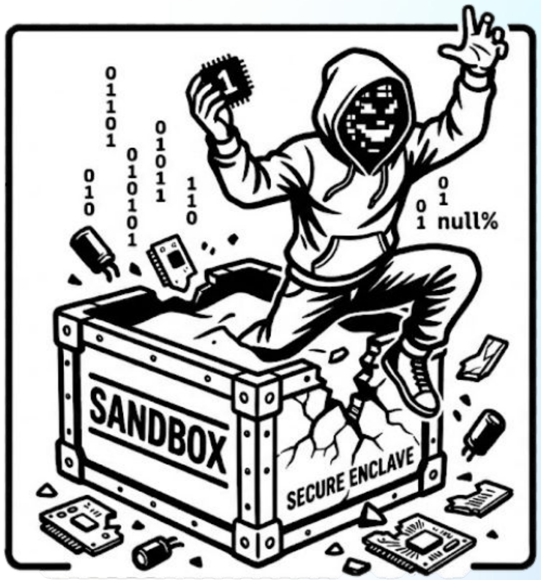
Criticals

CVE-2026-45607 – 8.4

CVE-2026-45641 – 8.4

CVE-2026-47652 – 8.2

Hyper-V sandbox escape



Criminally underrated.

Malicious code run in a guest VM can execute arbitrary code on the host.

Criticals

CVE-2025-10263 – 9.3 **ARM elevation of privilege**

Local memory attack vector allows escalation to SYSTEM

Overscored by being marked as No UI and no privileges required.

Criticals - Standard issue office RCE’s

CVE-2026-45456 – 8.4

CVE-2026-45458 – 8.4

CVE-2026-45461 – 8.4

CVE-2026-45472 – 8.4

CVE-2026-45474 – 8.4

CVE-2026-47635 – 8.4

CVE-2026-45463 – 8.4

CVE-2026-45460 – 4.7?

Office preview pane RCE’s

← Cute information disclosure vulnerability

The preview pane beatings will continue until morale improves.

Mythos - imminent release

- Has been delayed due to adding guardrails
- Poorly maintained open source libraries at greatest risk
- BigFix content release pipeline is turbocharged and ready for the flood

HCLSoftware

BigFix Compliance Analytics

- 2.0 patch 17 released
- New! CIS checklist for Microsoft Office

BigFix Scanner 11.0.42.1

- Security updates
  - Zlib 1.3.2
  - Golang 1.25

HCLSoftware