HCLSoftware

HCL BigFix

Patch Tuesday Webinar

September 2026

Agenda

01 Month at a glance

02 Vulnerability breakdown by type

03 Workstation TCP stack destroyed

04 No Hotpatch this month!

05 BigFix content support for Ubuntu Pro

Microsoft CVE’s at a Glance in September 2026

Total CVEs

966

Active vulnerabilities tracked and addressed across systems this month.

Zero days

2

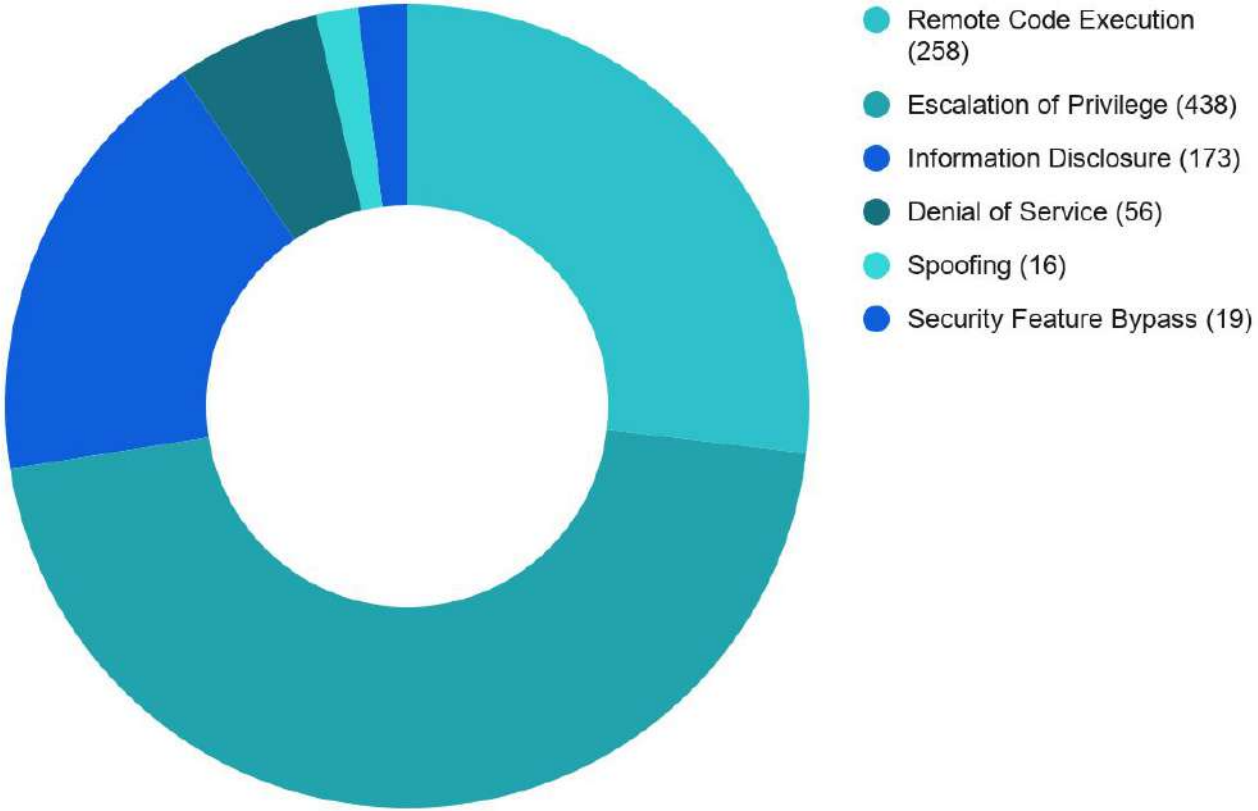
Zero-day exploits discovered.

Acceleration Focus

Patch these devices ASAP!

- **Any device with an IP address**
- **SQL servers**
- **DNS Servers**
- **Domain controllers**
- **Clustered Servers**

This Month’s Vulnerability Breakdown by Type



All Local Zero Days

Local elevation of privilege by an authorized attacker

CVE-2026-81963 **Score: 7.8**

Windows Update Elevation of Privilege

Allows an authorized attacker to elevate system privileges locally through the update service.

CVE-2026-81963 **Score: 7.8**

Windows Advanced Local Procedure Call EOP

Allows an authorized attacker to elevate system privileges locally through the LPC service.

HCLSoftware

Apocalypse Level Client Criticals

Three ultra-high severity remote code execution (RCE) vulnerabilities demanding immediate mitigation.

CVE-2025-729839.8 CRITICAL

Windows ICS RCE

Internet Connection Sharing

Unauthenticated, no User Interaction required. Single packet RCE against the ICS service.

CVE-2025-729829.8 CRITICAL

Windows Netlogon RCE

Netlogon Daemon

Unauthenticated, no User Interaction required. Single packet RCE against the default Windows netlogon service.

CVE-2025-730099.8 CRITICAL

Windows SSTP RCE

Secure Socket Tunneling

Secure Socket Tunneling Protocol is the native VPN protocol. Vulnerability allows an unauthenticated attacker to execute code.

HCLSoftware

Criticals

CVE-2025-69730 – 9.8 **Windows RNDIS RCE**

Remote Network Driver Interface allows USB devices to be used as network devices.

Any computer with a USB network device is vulnerable to instant RCE.

Lateral network attack Criticals

These services are vulnerable to RCE from attackers inside your network making arbitrary calls against network endpoints.

CVE-2025-69769 9.8 **Windows HTTP Print Provider RCE**

CVE-2025-69431 9.8 **Telnet Client RCE**

CVE-2025-69463 9.8 **Windows NTFS RCE**

CVE-2025-69408 9.8 **Windows Media Foundation**

CVE-2025-69715 9.8 **DirectShow RCE**

HCLSoftware

Server Component Criticals

CVE-2025-69730 (9.8) CVE-2025-72987 (8.1)

Windows DNS Server RCE

Use after free allows an unauthorized attacker to execute code as the DNS server.

CVE-2025-69712 (8.8)

Windows Key Distribution Center RCE

Any authorized attacker on the domain can execute code in the context of the domain controller.

CVE-2025-73010 (9.8)

Microsoft Failover Cluster RCE

Windows Server in a failover cluster can be taken over with no UI or Authentication.

CVE-2025-73025 (9.8)

Windows iSCSI Security Feature Bypass

Vulnerable to unauthorized storage access via the iSCSI target service.

exists running service "WinTarget"

HCLSoftware

Critical Vulnerabilities

SQL Server RCE

An authorized attacker can submit a query that triggers a wide array of memory corruption or a buffer overflow vulnerabilities, allowing for code execution.

Associated CVEs & Severity

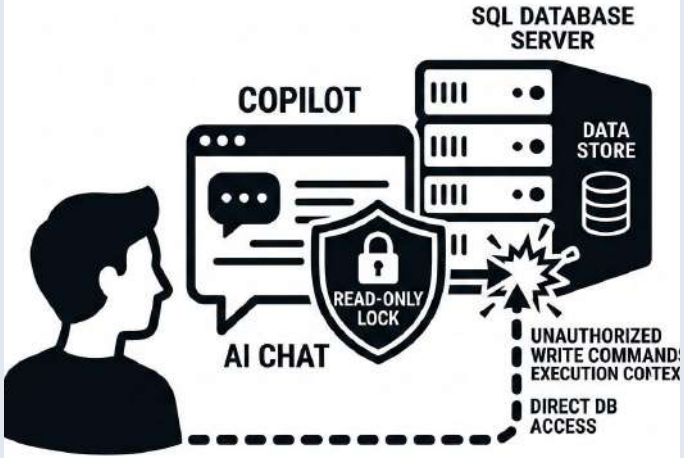
CVE-2025-67378 **Score: 8.5 (Critical)**

CVE-2025-67631 **Score: 8.8 (Critical)**

CVE-2025-67636 **Score: 8.5 (Critical)**

CVE-2025-67643 **Score: 8.8 (Critical)**

Critical Vulnerabilities



Microsoft SQL Server Elevation of Privilege

Copilot for SQL - an attacker can bypass the Copilot level read-only flag to run a command in the full user context with potential write access.

Associated CVE & Severity

CVE-2025-65669 Score: 9.6 (Critical)

Criticals

CVE-2025-77493 – 9.8 **Microsoft Office Outlook RCE**

Outlook native vulnerability that allows an attacker to run code from the reading pane with zero clicks from the user.

HCLSoftware

Criticals

CVE-2025-66302 – 9.8 **Skype for Business RCE**

Control of a file name or path allows an attacker to execute arbitrary code on the server.

Criticals

CVE-2025-65772 – 8.8

Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability

A low privileged Dynamics user can execute arbitrary code over the network in the context of the Dynamics server account.

HCLSoftware

New! Support for Ubuntu Pro 18.04 and 20.04

Ubuntu Pro 18.04 Support

Site Name: Patches for Ubuntu Pro 1804
Supported Repos: bionic-infra and bionic-apps

Ubuntu Pro 20.04 Support

Site Name: Patches for Ubuntu Pro 2004
Supported Repos: focal-infra and focal-apps

Required BigFix Entitlements

Access to these new sites requires entitlement to any of the following licenses:

- **BigFix** Remediate
- **BigFix** Lifecycle
- **BigFix** Compliance
- **BigFix** Workspace / Workspace+
- **BigFix** Enterprise / Enterprise+

HCLSoftware