Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's March 2026 Patch Tuesday

Date of Publication	Admiralty Code	TA Number
March 12, 2026	A1	TA2026067

Summary

First Seen: March 10, 2026
Affected Platforms: Microsoft SQL Server, Windows Kerberos, Windows Update Service, Microsoft Office, Microsoft SharePoint, Google Chromium, and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-26127	.NET Denial of Service Vulnerability	.NET 9.0	✗	✗	✓
CVE-2026-21262	SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server 2025, 2022, 2019, 2017, 2016	✗	✗	✓
CVE-2026-23668	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2017, 2022; Windows 10 Version 1607, 1809; Windows 11 Version 23H2	✗	✗	✓
CVE-2026-24289	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2017, 2022; Windows 10 Version 1607, 1809; Windows 11 Version 23H2	✗	✗	✓
CVE-2026-24291	Windows Accessibility Infrastructure (ATBroker.exe) Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2017, 2022; Windows 10 Version 1607, 1809; Windows 11 Version 23H2	✗	✗	✓
CVE-2026-24294	Windows SMB Server Elevation of Privilege Vulnerability	Windows 11 Version 23H2, 25H2; Windows Server 2025; Windows 10 Version 22H2	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-25187	Winlogon Elevation of Privilege Vulnerability	Windows 11 version 26H1; Windows Server 2012, 2016; Windows 10 Version 1607	✗	✗	✓
CVE-2026-26132	Windows Kernel Elevation of Privilege Vulnerability	Windows 11 version 26H1; Windows Server 2025, 2022; Windows 10 Version 22H2	✗	✗	✓
CVE-2026-21536	Microsoft Devices Pricing Program Remote Code Execution Vulnerability	Microsoft Devices Pricing Program	✗	✗	✓
CVE-2026-25188	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2025; Windows 10 Version 1607; Windows 11 Version 24H2	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1189: Drive-by Compromise	
Execution	T1059: Command and Scripting Interpreter	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
Defense Evasion	T1036: Masquerading	
	T1218: System Binary Proxy Execution	
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
	T1543: Create or Modify System Process	T1543.003: Windows Service
Credential Access	T1552: Unsecured Credentials	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation

Vulnerability Details

#1

Microsoft's March 2026 Patch Tuesday delivers an extensive batch of security updates, addressing 83 vulnerabilities across its product ecosystem. These include 8 rated critical, 75 marked important in severity. The vulnerabilities span various categories: 46 Elevation of Privilege, 18 Remote Code Execution, 10 Information Disclosure, 4 Denial of Service, 4 Spoofing, and 1 Security Feature Bypass. Beyond its own products, Microsoft also released patches for 10 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 93. Notably, 10 of these CVEs are considered at risk of active exploitation, underscoring the urgency of deploying patches promptly.

#2

Among the standout flaws is CVE-2026-26127, a denial-of-service (DoS) vulnerability affecting Microsoft .NET versions 9.0 and 10.0 running on Windows, macOS, and Linux. The flaw stems from improper handling of certain inputs within the .NET runtime, allowing an unauthenticated remote attacker to trigger a crash in affected applications. While the primary risk is application unavailability, a secondary risk exists in other attack types being attempted during a service restart window. This vulnerability was publicly disclosed before the patch was made available, though no active exploitation has been confirmed.

#3

CVE-2026-21262 is an elevation of privilege vulnerability in Microsoft SQL Server 2016 and later editions. The root cause is improper access control within the SQL Server engine, which allows an authorized, network-based attacker to escalate their privileges to the sysadmin database role. This is significant because sysadmin access grants full administrative control over the SQL Server instance, including the ability to execute operating system commands via xp_cmdshell. The vulnerability was publicly disclosed before patching, while exploitation is less likely, its network-exploitable nature and the severity of the privilege level it grants make it a high-priority remediation target.

#4

CVE-2026-24294 is an elevation-of-privilege vulnerability in the Windows SMB Server component, stemming from improper authentication logic in the SMB implementation. A locally authenticated attacker could exploit the flaw to gain SYSTEM privileges. Given the ubiquity of SMB in enterprise environments for file sharing and network communication, this vulnerability represents a meaningful lateral movement risk in environments where SMB is accessible across workstation segments.

#5

CVE-2026-25188 is an elevation of Privilege Vulnerability in the Windows Telephony Service (TAPI). The vulnerability, resulting from a heap-based buffer overflow, allows an attacker to send specially crafted telephony-related requests to the service, causing it to write data beyond the boundaries of an allocated heap buffer. Successful exploitation could result in privilege escalation of the Telephony Service process. Organizations that expose telephony services or use TAPI-integrated applications, particularly in regulated sectors, should prioritize patching this vulnerability promptly.

Recommendations

Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.

Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.

Prioritize Exploitable Vulnerabilities in this advisory, CVE-2026-26127, CVE-2026-23668, CVE-2026-21262, CVE-2026-24289, CVE-2026-24291, CVE-2026-24294, CVE-2026-25187, and CVE-2026-26132." Security teams should treat patching these flaws as urgent priorities within their patch deployment windows, recognizing that these vulnerabilities feature low attack complexity and require no user interaction, making them attractive to post-exploitation toolkits and automated exploitation frameworks.

Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.

Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Harden SQL Server Deployments in response to CVE-2026-21262, administrators should immediately audit SQL Server instances for network exposure and ensure that only authorized and minimally privileged accounts have network access to the database engine. Where feasible, disable or restrict the xp_cmdshell extended stored procedure and enable SQL Server Audit to detect unexpected privilege escalation events. Apply the March 2026 SQL Server cumulative updates across all instances of SQL Server 2016 through the latest release.

Restrict and Monitor SMB Access Given the elevation of privilege vulnerability in Windows SMB Server (CVE-2026-24294), organizations should review SMB exposure across their network environments. Where possible, restrict SMB access between workstation segments using firewall rules and network micro-segmentation. Monitor for anomalous SMB authentication attempts or unusual SYSTEM-level process spawning on SMB-facing hosts as an indicator of potential exploitation.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2026-20967	System Center Operations Manager (SCOM) Elevation of Privilege Vulnerability	Connected Devices Platform Service (Cdpsvc)	Elevation of Privilege
CVE-2026-21262	SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
CVE-2026-21536	Microsoft Devices Pricing Program Remote Code Execution Vulnerability	Microsoft Devices Pricing Program	Remote Code Execution
CVE-2026-23651	Microsoft ACI Confidential Containers Elevation of Privilege Vulnerability	Azure Compute Gallery	Elevation of Privilege
CVE-2026-23654	GitHub: Zero Shot SCFoundation Remote Code Execution Vulnerability	GitHub Repo: zero-shot-scfoundation	Remote Code Execution
CVE-2026-23656	Windows App Installer Spoofing Vulnerability	Windows App Installer	Spoofing
CVE-2026-23660	Windows Admin Center in Azure Portal Elevation of Privilege Vulnerability	Azure Portal Windows Admin Center	Elevation of Privilege
CVE-2026-23661	Azure IoT Explorer Information Disclosure Vulnerability	Azure IoT Explorer	Information Disclosure
CVE-2026-23662	Azure IoT Explorer Information Disclosure Vulnerability	Azure IoT Explorer	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-23664	Azure IoT Explorer Information Disclosure Vulnerability	Azure IoT Explorer	Information Disclosure
CVE-2026-23665	Linux Azure Diagnostic extension (LAD) Elevation of Privilege Vulnerability	Azure Linux Virtual Machines	Elevation of Privilege
CVE-2026-23667	Broadcast DVR Elevation of Privilege Vulnerability	Broadcast DVR	Elevation of Privilege
CVE-2026-23668	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2026-23669	Windows Print Spooler Remote Code Execution Vulnerability	Windows Print Spooler Components	Remote Code Execution
CVE-2026-23671	Windows Bluetooth RFCOM Protocol Driver Elevation of Privilege Vulnerability	Windows Bluetooth RFCOM Protocol Driver	Elevation of Privilege
CVE-2026-23672	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	Windows Universal Disk Format File System Driver (UDFS)	Elevation of Privilege
CVE-2026-23673	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	Windows Resilient File System (ReFS)	Elevation of Privilege
CVE-2026-23674	MapUrlToZone Security Feature Bypass Vulnerability	Windows MapUrlToZone	Security Feature Bypass
CVE-2026-24282	Push message Routing Service Elevation of Privilege Vulnerability	Push Message Routing Service	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-24283	Multiple UNC Provider Kernel Driver Elevation of Privilege Vulnerability	Windows File Server	Elevation of Privilege
CVE-2026-24285	Win32k Elevation of Privilege Vulnerability	Windows Win32K	Elevation of Privilege
CVE-2026-24287	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-24288	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Windows Mobile Broadband	Remote Code Execution
CVE-2026-24289	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-24290	Windows Projected File System Elevation of Privilege Vulnerability	Windows Projected File System	Elevation of Privilege
CVE-2026-24291	Windows Accessibility Infrastructure (ATBroker.exe) Elevation of Privilege Vulnerability	Windows Accessibility Infrastructure (ATBroker.exe)	Elevation of Privilege
CVE-2026-24292	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Connected Devices Platform Service (Cdpsvc)	Elevation of Privilege
CVE-2026-24293	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-24294	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-24295	Windows Device Association Service Elevation of Privilege Vulnerability	Windows Device Association Service	Elevation of Privilege
CVE-2026-24296	Windows Device Association Service Elevation of Privilege Vulnerability	Windows Device Association Service	Elevation of Privilege
CVE-2026-24297	Windows Kerberos Security Feature Bypass Vulnerability	Windows Kerberos	Security Feature Bypass
CVE-2026-25165	Performance Counters for Windows Elevation of Privilege Vulnerability	Windows Performance Counters	Elevation of Privilege
CVE-2026-25166	Windows System Image Manager Assessment and Deployment Kit (ADK) Remote Code Execution Vulnerability	Windows System Image Manager	Remote Code Execution
CVE-2026-25167	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2026-25168	Windows Graphics Component Denial of Service Vulnerability	Microsoft Graphics Component	Denial of Service
CVE-2026-25169	Windows Graphics Component Denial of Service Vulnerability	Microsoft Graphics Component	Denial of Service
CVE-2026-25170	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V	Elevation of Privilege
CVE-2026-25171	Windows Authentication Elevation of Privilege Vulnerability	Windows Authentication Methods	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-25172	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2026-25173	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2026-25174	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability	Windows Extensible File Allocation	Elevation of Privilege
CVE-2026-25175	Windows NTFS Elevation of Privilege Vulnerability	Windows NTFS	Elevation of Privilege
CVE-2026-25176	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-25177	Active Directory Domain Services Elevation of Privilege Vulnerability	Active Directory Domain Services	Elevation of Privilege
CVE-2026-25178	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-25179	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-25180	Windows Graphics Component Information Disclosure Vulnerability	Microsoft Graphics Component	Information Disclosure
CVE-2026-25181	GDI+ Information Disclosure Vulnerability	Windows GDI+	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-25185	Windows Shell Link Processing Spoofing Vulnerability	Windows Shell Link Processing	Spoofing
CVE-2026-25186	Windows Accessibility Infrastructure (ATBroker.exe) Information Disclosure Vulnerability	Windows Accessibility Infrastructure (ATBroker.exe)	Information Disclosure
CVE-2026-25187	Winlogon Elevation of Privilege Vulnerability	Winlogon	Elevation of Privilege
CVE-2026-25188	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-25189	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-25190	GDI Remote Code Execution Vulnerability	Windows GDI	Remote Code Execution
CVE-2026-26105	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint	Spoofing
CVE-2026-26106	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-26107	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-26108	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-26109	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-26110	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-26111	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2026-26112	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-26113	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-26114	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-26115	SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
CVE-2026-26116	SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
CVE-2026-26117	Arc Enabled Servers - Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Windows Virtual Machine Agent	Elevation of Privilege
CVE-2026-26118	Azure MCP Server Tools Elevation of Privilege Vulnerability	Azure MCP Server	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-26121	Azure IOT Explorer Spoofing Vulnerability	Azure IoT Explorer	Spoofing
CVE-2026-26122	Microsoft ACI Confidential Containers Information Disclosure Vulnerability	Azure Compute Gallery	Information Disclosure
CVE-2026-26123	Microsoft Authenticator Information Disclosure Vulnerability	Microsoft Authenticator	Information Disclosure
CVE-2026-26124	Microsoft ACI Confidential Containers Elevation of Privilege Vulnerability	Azure Compute Gallery	Elevation of Privilege
CVE-2026-26125	Payment Orchestrator Service Elevation of Privilege Vulnerability	Payment Orchestrator Service	Elevation of Privilege
CVE-2026-26127	.NET Denial of Service Vulnerability	.NET	Denial of Service
CVE-2026-26128	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2026-26130	ASP.NET Core Denial of Service Vulnerability	ASP.NET Core	Denial of Service
CVE-2026-26131	.NET Elevation of Privilege Vulnerability	.NET	Elevation of Privilege
CVE-2026-26132	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-26134	Microsoft Office Elevation of Privilege Vulnerability	Microsoft Office	Elevation of Privilege
CVE-2026-26141	Hybrid Worker Extension (Arc-enabled Windows VMs) Elevation of Privilege Vulnerability	Azure Arc	Elevation of Privilege
CVE-2026-26144	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2026-26148	Microsoft Azure AD SSH Login extension for Linux Elevation of Privilege Vulnerability	Azure Entra ID	Elevation of Privilege
CVE-2026-26030	GitHub: CVE-2026-26030 Microsoft Semantic Kernel InMemoryVectorStore filter functionality vulnerable	Microsoft Semantic Kernel Python SDK	Remote Code Execution
CVE-2026-3536	Chromium Integer overflow in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3538	Chromium Integer overflow in Skia Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3539	Chromium Object lifecycle issue in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3540	Chromium Inappropriate implementation in WebAudio Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-3541	Chromium Inappropriate implementation in CSS Vulnerability	Microsoft Edge (Chromium-based)	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-3542	Chromium Inappropriate implementation in WebAssembly Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3543	Chromium Inappropriate implementation in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3544	Chromium Heap buffer overflow in WebCodecs Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-3545	Chromium Insufficient data validation in Navigation Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

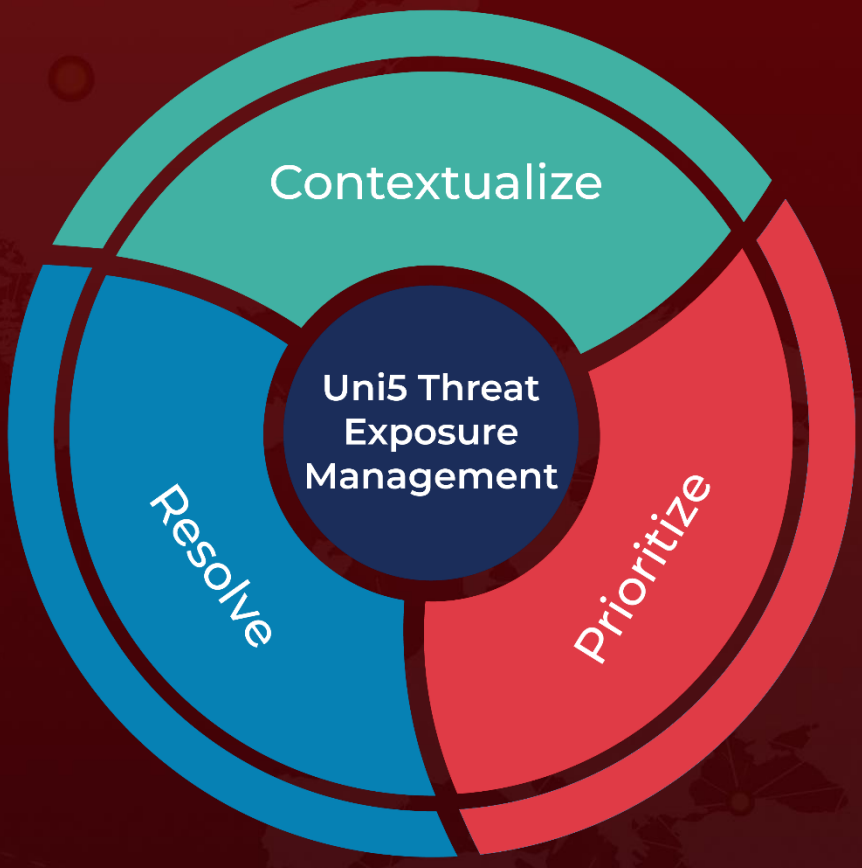
References

https://msrc.microsoft.com/update-guide/releaseNote/2026-Mar

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 12, 2026 • 1:00 AM

More at www.hivepro.com