July Patch Tuesday Unleashes a Torrent of Updates

Microsoft fixes 138 bugs in Windows and other products this month

Written by Andrew Brandt

JULY 09, 2024

THREAT RESEARCH AZURE DATABASE DYNAMICS365 EOP MICROSOFT MICROSOFT SQL SERVER MS-SQL OFFICE365 PATCH TUESDAY PEOPLE RATING RCE SOPHOS X-OPS SQL SERVER WINDOWS

With the information security industry's two largest conferences (Black Hat Briefings and Def Con) set to happen in less than a month, Microsoft pulled out all the stops and, for July, nearly tripled the number of patches they released in

June for problems discovered in Windows, Office, and software that runs under various server and cloud platforms.

The single product most prominently featured in the hot summer flood of fixes is Microsoft SQL Server. The Microsoft SQL Server Native Client component of this month's update will fix 38 distinct remote code execution bugs in the OLE database driver. An attacker might invoke any of the bugs in the OLE DB driver by tricking an authenticated account into connecting to a malicious SQL Server database; The exploit happens when that malicious database returns data that triggers arbitrary code execution on the client.

Remote code execution bugs comprise the largest proportion of this month's fixes, with the 59 RCEs making up more than 43% of the total number of problems this month's cumulative update will resolve. Microsoft rates five of the RCE vulnerabilities at the highest severity level of "critical," including bugs that affect SharePoint Server, Windows Remote Desktop Licensing Service, and the Windows Codec library.

July's list of vulnerabilities includes 13 that Microsoft considers "more likely" exploitable than the rest, including the critical bugs in SharePoint Server and the Windows Codec library. Thankfully, Microsoft says only one of the bugs fixed this month have been exploited or have been made public – CVE-2024-38080, a privilege escalation exploit in the Windows Hyper-V hypervisor for virtual machines. Six of this month's bugs are detectable through Sophos IPS rules in the XGS Firewall; Information about these are included in a table at the end of this article.

While the majority of these vulnerabilities were reported directly to Microsoft, some of the bug reports originated with outside organizations, who responsibly disclosed the information to Microsoft. Adobe reported CVE-2024-34122, an as-yet unexploited remote code execution vulnerability in the Chromium version of the Edge browser that was fixed prior to Patch Tuesday with the release of version 126.0.2592.81 on June 27. The CERT/CC at Carnegie Mellon University reported CVE-2024-3596, a forgery vulnerability that affects many operating systems' implementation of the RADIUS protocol (RFC 2865) over UDP. Finally, Intel reported CVE-2024-37985, a weakness in the ARM processor family that,

for Microsoft customers, only affects computers running Windows 11 version 22H2 on a 64-bit ARM (ARM64) CPU.

By the numbers

Total Microsoft CVEs: 138

Total Edge / Chrome advisory issues covered in update: 1

Total non- Microsoft advisory issues covered in update: 4

Total Adobe issues covered in update: 1

Publicly disclosed: 1

Exploited: 1

Severity

Critical: 5

Important: 132

Moderate: 1

Impact:

Remote Code Execution: 59

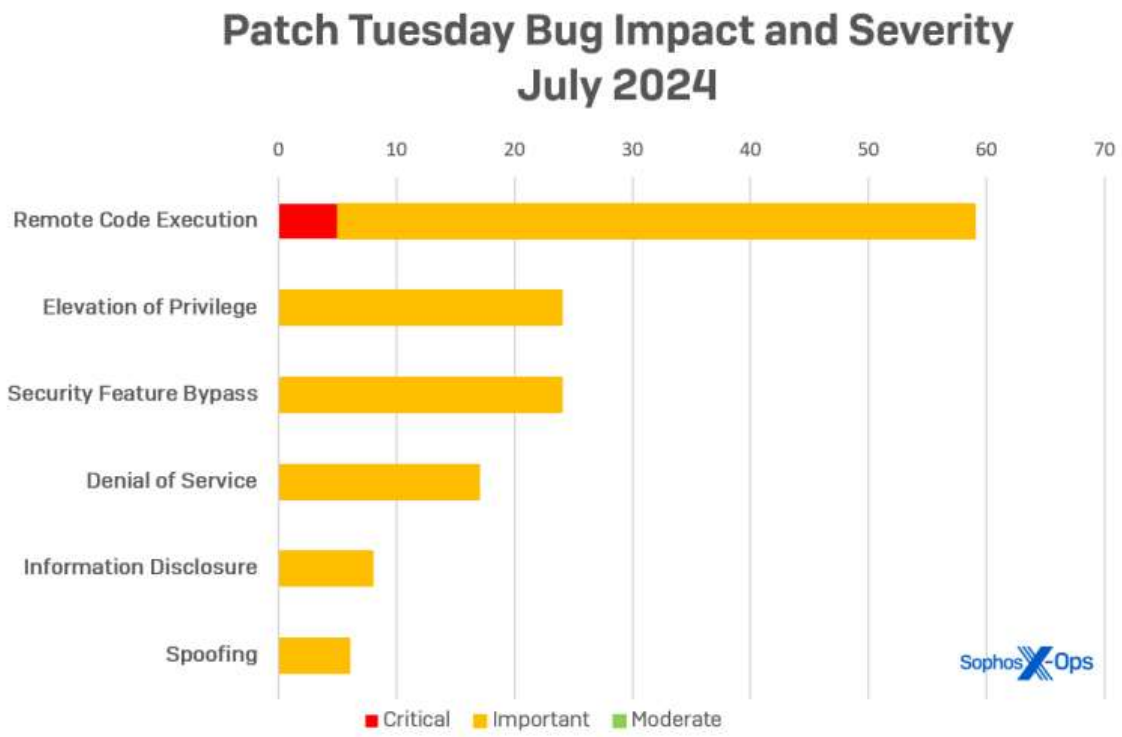
Elevation of Privilege: 24

Security Feature Bypass: 24

Denial of Service: 17

Information Disclosure: 8

Spoofing: 7



July's Patch Tuesday addresses 138 bugs in six vulnerability categories

Products

Windows (including .NET and ASP.NET): 87

Microsoft SQL Server: 38

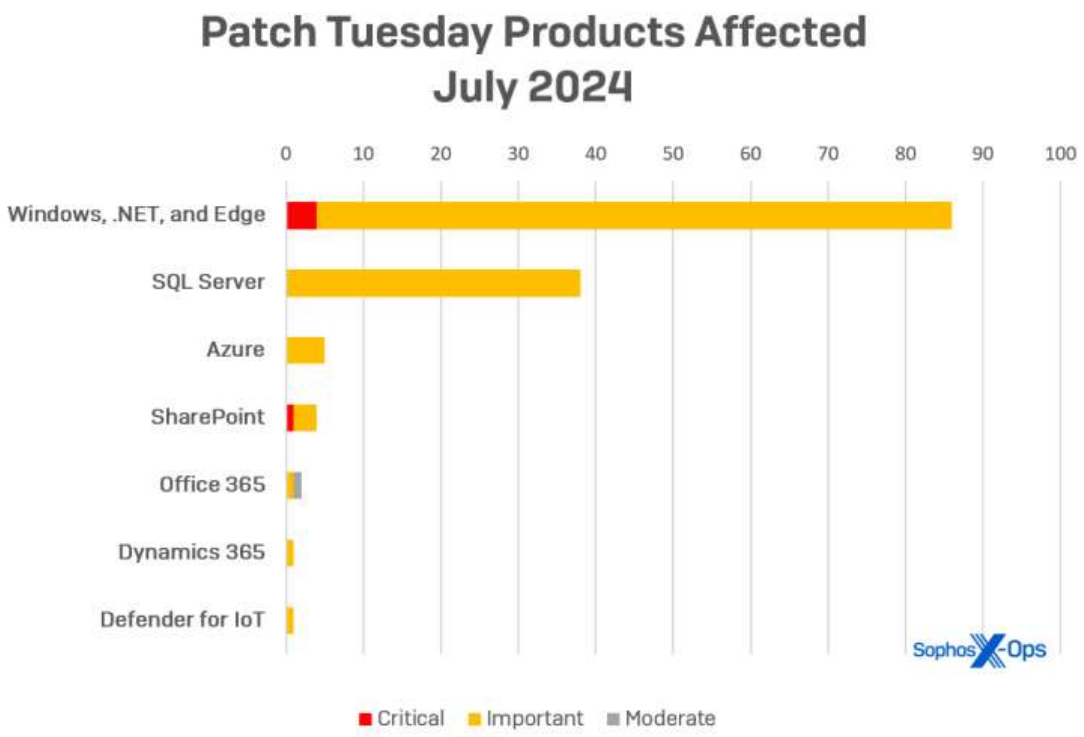
Azure: 5

SharePoint: 4

Office: 2

Dynamics 365: 1

Microsoft Defender for IoT: 1



Windows accounts for almost two-thirds of July's patches

Notable July updates

In addition to the issues discussed above, a few specific items merit attention.

Microsoft SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability

Microsoft ticks off 38 CVEs this month in fixes to its mature database family. There are too many CVE numbers to list them all here, but the patches all seem to address various permutations of the same general exploit process: If an attacker tricks an authenticated user of a legitimate MS-SQL database server into connecting to their malicious MS-SQL Server, arbitrary code on this malicious server would then propagate back up from the server to the client computer, and execute on the client.

The convoluted exploit requires that the hypothetical attackers do some work in advance, building out a database server that contains malicious content inside its tables. And, of course, it requires the targeted user not to have updated their SQL Server client software with this month's cumulative update, and that the

attackers identify and target a database admin, and successfully social-engineer them. Don't be that unicorn.

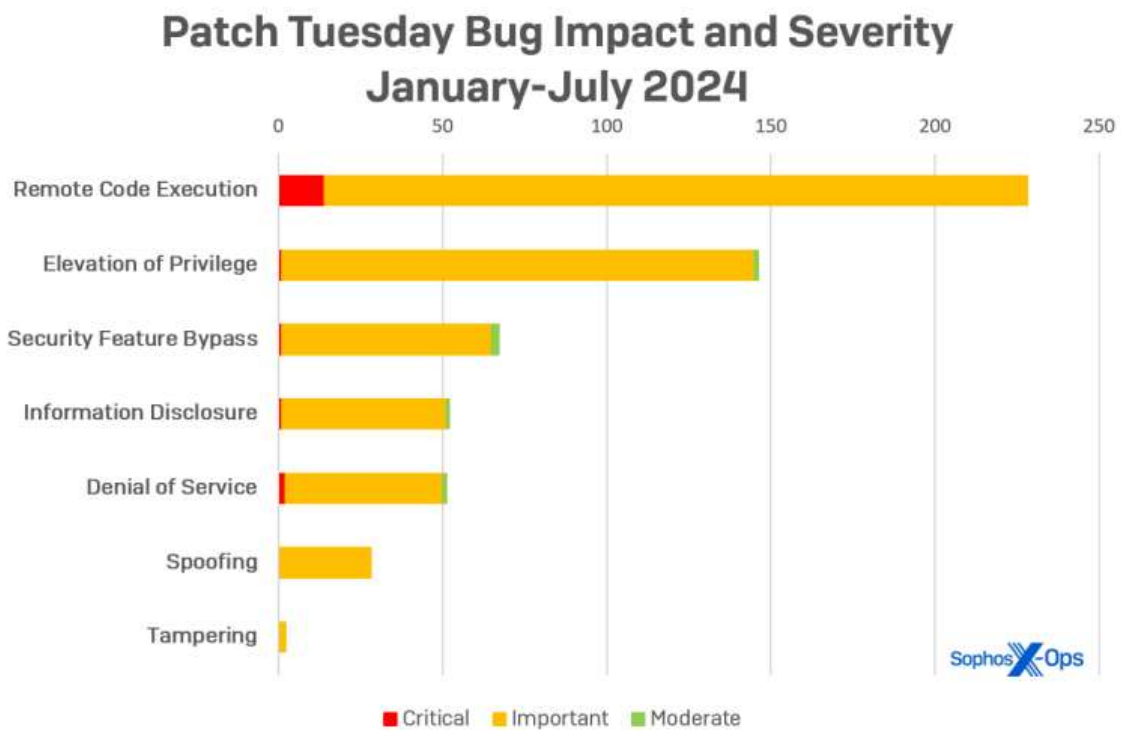
CVE-2024-38060 – Microsoft Windows Codecs Library Remote Code Execution Vulnerability

In the year 1986, the world was introduced to a pair of cowboy fighter pilots (ahem, naval aviators) in *Top Gun*. Less well known, but still *Alive And Kicking* (like the song released the same year by Simple Minds), the TIFF image file format also was introduced that year by Aldus Corporation, now known as Adobe.

This CVE addresses a critical, easily exploitable vulnerability specific to this 38-year-old file format. A specially-crafted, malicious TIFF file, uploaded to a vulnerable server, could have triggered the server that receives the file to execute malicious code embedded in the TIFF file. Patch your servers to take them out of the danger zone.

CVE-2024-38032 – Microsoft Xbox Remote Code Execution Vulnerability

Users of the Xbox gaming console who also happen to have a wireless adapter, and connect wirelessly to their local network, should beware of strangers lurking on their network who can attack these devices. The (so far) hypothetical threat is that someone who is connected to your wireless network can send a malicious network packet to the Xbox, one that could execute an arbitrary command. The attacker has to be connected to the same network as the Xbox, so it's another good reason not to invite any threat actors to your WLAN party.



Heading into summer, RCE bugs comprise nearly 40% of the total patched bugs so far in calendar year 2024

Sophos protections

CVE	Sophos Intercept X/Endpoint IPS	Sophos XGS Firewall
CVE-2024-38021	sid:2309849, sid:2309850	sid:2309849, sid:2309850
CVE-2024-38052	Exp/2438052-A	
CVE-2024-38054	Exp/2438054-A	
CVE-2024-38059	Exp/2438059-A	
CVE-2024-38080	Exp/2438080-A	
CVE-2024-38085	Exp/2438085-A	

As you can every month, if you don't want to wait for your system to pull down Microsoft's updates itself, you can download them manually from the Microsoft Update Catalog website. Run the **winver.exe** tool to determine which build of Windows you're running, then download the Cumulative Update package for your specific system's architecture and build number.

Appendix A: Vulnerability Impact and Severity

This is a list of July patches sorted by impact, then sub-sorted by severity. Each list is further arranged by CVE.

Denial of Service (17 CVEs)

Important severity

CVE-2024-30105	.NET Denial of Service Vulnerability
CVE-2024-35270	Windows iSCSI Service Denial of Service Vulnerability
CVE-2024-38015	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2024-38027	Windows Line Printer Daemon Service Denial of Service Vulnerability
CVE-2024-38031	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38048	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability
CVE-2024-38067	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38068	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38071	Windows Remote Desktop Licensing Service Denial of Service Vulnerability

CVE-2024-38072	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38073	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38091	Microsoft WS-Discovery Denial of Service Vulnerability
CVE-2024-38095	.NET Denial of Service Vulnerability
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38101	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38102	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38105	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability

Elevation of Privileges (24 CVEs)

Important severity

CVE-2024-21417	Windows CoreMessaging Elevation of Privileges Vulnerability
CVE-2024-30079	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2024-35261	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability
CVE-2024-38013	Microsoft Windows Server Backup Elevation of Privilege Vulnerability

CVE-2024-38022	Windows Image Acquisition Elevation of Privilege Vulnerability
CVE-2024-38033	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38034	Windows Filtering Platform Elevation of Privilege Vulnerability
CVE-2024-38043	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38047	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38050	Windows Workstation Service Elevation of Privilege Vulnerability
CVE-2024-38052	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38054	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38057	Microsoft Streaming Service Elevation of Privilege Vulnerability
CVE-2024-38059	Win32k Elevation of Privilege Vulnerability
CVE-2024-38061	Active Directory Certificate Services Elevation of Privilege Vulnerability
CVE-2024-38062	Windows Clip Service Elevation of Privilege Vulnerability
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability

CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
CVE-2024-38085	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2024-38089	Microsoft Defender for IoT Elevation of Privilege Vulnerability
CVE-2024-38092	Azure CycleCloud Elevation of Privilege Vulnerability
CVE-2024-38100	Windows File Explorer Elevation of Privilege Vulnerability

Information Disclosure (9 CVEs)

Important severity

CVE-2024-30061	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability
CVE-2024-30071	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-32987	Microsoft SharePoint Server Information Disclosure Vulnerability
CVE-2024-37985	Intel ARM: Systematic Identification and Characterization of Proprietary Prefetchers
CVE-2024-38017	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-38041	Windows Kernel Information Disclosure Vulnerability
CVE-2024-38055	Microsoft Windows Codecs Library Information Disclosure Vulnerability

CVE-2024-38056	Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2024-38064	Windows TCP/IP Information Disclosure Vulnerability

Remote Code Execution (59 CVEs)

Critical severity

CVE-2024-38023	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2024-38060	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2024-38074	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38076	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38077	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

Important severity

CVE-2024-20701	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21303	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21308	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21317	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21331	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability

CVE-2024-21332	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21333	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21335	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21373	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21398	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21414	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21415	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21425	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21428	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-21449	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-28928	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-30013	Windows MultiPoint Services Remote Code Execution Vulnerability
CVE-2024-35256	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-35264	.NET and Visual Studio Remote Code Execution Vulnerability
CVE-2024-35271	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability

CVE-2024-35272	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37318	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37319	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37320	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37321	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37322	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37323	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37324	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37326	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37327	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37328	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37329	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37330	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37331	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37332	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability

CVE-2024-37333	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-37334	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37336	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-38019	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability
CVE-2024-38021	Microsoft Office Remote Code Execution Vulnerability
CVE-2024-38024	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2024-38025	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability
CVE-2024-38028	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability
CVE-2024-38032	Microsoft Xbox Remote Code Execution Vulnerability
CVE-2024-38044	DHCP Server Service Remote Code Execution Vulnerability
CVE-2024-38049	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability
CVE-2024-38051	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
CVE-2024-38078	Xbox Wireless Adapter Remote Code Execution Vulnerability
CVE-2024-38086	Azure Kinect SDK Remote Code Execution Vulnerability

CVE-2024-38087	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-38088	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability
CVE-2024-38094	Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2024-38104	Windows Fax Service Remote Code Execution Vulnerability

Security Feature Bypass (24 CVEs)

Important severity

CVE-2024-26184	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28899	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-30098	Windows Cryptographic Services Security Feature Bypass Vulnerability
CVE-2024-37969	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37970	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37971	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37972	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37973	Secure Boot Security Feature Bypass Vulnerability

CVE-2024-37974	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37975	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37977	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37978	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37981	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37984	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37986	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37987	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37988	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37989	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38010	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38011	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38058	BitLocker Security Feature Bypass Vulnerability
CVE-2024-38065	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability

CVE-2024-38070	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability

Spoofing (7 CVEs)

Important severity

CVE-2024-30081	Windows NTLM Spoofing Vulnerability
CVE-2024-35266	Azure DevOps Server Spoofing Vulnerability
CVE-2024-35267	Azure DevOps Server Spoofing Vulnerability
CVE-2024-38112	Windows MSHTML Platform Spoofing Vulnerability
CVE-2024-38030	Windows Themes Spoofing Vulnerability

Moderate severity

CVE-2024-38020	Microsoft Outlook Spoofing Vulnerability

Appendix B: Exploitability

This is a list of the July CVEs judged by Microsoft to be more likely to be exploited in the wild within the first 30 days post-release. This month's updates do not address any vulnerabilities Microsoft knows are being exploited.

Exploitation more likely within the next 30 days

CVE-2024-38021	Microsoft Office Remote Code Execution Vulnerability
CVE-2024-38023	Microsoft SharePoint Server Remote Code Execution Vulnerability

CVE-2024-38024	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2024-38052	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38054	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38059	Win32k Elevation of Privilege Vulnerability
CVE-2024-38060	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2024-38085	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2024-38094	Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38100	Windows File Explorer Elevation of Privilege Vulnerability

Appendix C: Products Affected

This is a list of July's patches sorted by product family, then sub-sorted by severity. Each list is further arranged by CVE. Patches that are shared among

multiple product families are listed multiple times, once for each product family.

Windows (86 CVEs)

Critical severity	
CVE-2024-38060	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2024-38074	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38076	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38077	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
Important severity	
CVE-2024-21417	Windows Text Services Framework Elevation of Privileges Vulnerability
CVE-2024-26184	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28899	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-30013	Windows MultiPoint Services Remote Code Execution Vulnerability
CVE-2024-30071	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-30079	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2024-30081	Windows NTLM Spoofing Vulnerability
CVE-2024-30098	Windows Cryptographic Services Security Feature Bypass Vulnerability

CVE-2024-30105	.NET Denial of Service Vulnerability
CVE-2024-35264	ASP.NET Remote Code Execution Vulnerability
CVE-2024-35270	Windows iSCSI Service Denial of Service Vulnerability
CVE-2024-37969	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37970	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37971	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37972	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37973	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37974	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37975	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37977	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37978	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37981	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37984	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37986	Secure Boot Security Feature Bypass Vulnerability

CVE-2024-37987	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37988	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37989	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38010	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38011	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38013	Microsoft Windows Server Backup Elevation of Privilege Vulnerability
CVE-2024-38015	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2024-38017	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-38019	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability
CVE-2024-38022	Windows Image Acquisition Elevation of Privilege Vulnerability
CVE-2024-38025	Windows Performance Monitor Remote Code Execution Vulnerability
CVE-2024-38027	Windows Line Printer Daemon Service Denial of Service Vulnerability
CVE-2024-38028	Windows Performance Monitor Remote Code Execution Vulnerability
CVE-2024-38030	Windows Themes Spoofing Vulnerability
CVE-2024-38031	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability

CVE-2024-38032	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2024-38033	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38034	Windows Filtering Platform Elevation of Privilege Vulnerability
CVE-2024-38041	Windows Kernel Information Disclosure Vulnerability
CVE-2024-38043	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38044	DHCP Server Service Remote Code Execution Vulnerability
CVE-2024-38047	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38048	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability
CVE-2024-38049	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability
CVE-2024-38050	Windows Workstation Service Elevation of Privilege Vulnerability
CVE-2024-38051	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2024-38052	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
CVE-2024-38054	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38055	Microsoft Windows Codecs Library Information Disclosure Vulnerability

CVE-2024-38056	Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2024-38057	Microsoft Streaming Service Elevation of Privilege Vulnerability
CVE-2024-38058	BitLocker Security Feature Bypass Vulnerability
CVE-2024-38059	Win32k Elevation of Privilege Vulnerability
CVE-2024-38061	Active Directory Certificate Services Elevation of Privilege Vulnerability
CVE-2024-38062	Windows Clip Service Elevation of Privilege Vulnerability
CVE-2024-38064	Windows TCP/IP Information Disclosure Vulnerability
CVE-2024-38065	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability
CVE-2024-38067	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38068	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2024-38070	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
CVE-2024-38071	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38072	Windows Remote Desktop Licensing Service Denial of Service Vulnerability

CVE-2024-38073	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38078	XBox Wireless Adapter Remote Code Execution Vulnerability
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
CVE-2024-38085	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2024-38091	Microsoft WS-Discovery Denial of Service Vulnerability
CVE-2024-38095	.NET Denial of Service Vulnerability
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38100	Windows File Explorer Elevation of Privilege Vulnerability
CVE-2024-38101	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38102	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38104	Windows Fax Service Remote Code Execution Vulnerability
CVE-2024-38105	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability

SQL Server (38 CVEs)

Important severity

CVE-2024-20701	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21303	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21308	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21317	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21331	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21332	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21333	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21335	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21373	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21398	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21414	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21415	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21425	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVE-2024-21428	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-21449	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28928	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-35256	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-35271	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-35272	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37318	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37319	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37320	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37321	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37322	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37323	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37324	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37326	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37327	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVE-2024-37328	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37329	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37330	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37331	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37332	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37333	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37334	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-37336	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-38087	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-38088	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

Azure (5 CVEs)

Important severity

CVE-2024-35261	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability
CVE-2024-35266	Azure DevOps Server Spoofing Vulnerability

CVE-2024-35267	Azure DevOps Server Spoofing Vulnerability
CVE-2024-38086	Azure Kinect SDK Remote Code Execution Vulnerability
CVE-2024-38092	Azure CycleCloud Elevation of Privilege Vulnerability

SharePoint (4 CVEs)

Critical severity

CVE-2024-38023	Microsoft SharePoint Server Remote Code Execution Vulnerability

Important severity

CVE-2024-32987	Microsoft SharePoint Server Information Disclosure Vulnerability
CVE-2024-38024	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2024-38094	Microsoft SharePoint Remote Code Execution Vulnerability

Office 365 (2 CVEs)

Important severity

CVE-2024-38021	Microsoft Office Remote Code Execution Vulnerability

Moderate severity

CVE-2024-38020	Microsoft Outlook Spoofing Vulnerability

Microsoft Dynamics 365 (on-prem)

Important severity

CVE-2024-30061	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability

Microsoft Defender for IoT (1 CVE)

Important severity

CVE-2024-38089	Microsoft Defender for IoT Elevation of Privilege Vulnerability

About the Author

Andrew Brandt

Sophos X-Ops Principal Researcher Andrew Brandt blends a 20-year journalism background with deep, retrospective analysis of malware infections, ransomware, and cyberattacks as the editor of SophosLabs Uncut. His work with the Labs team helps Sophos protect its global customers, and alerts the world about notable criminal behavior and activity, whether it's normal or novel. Follow him at @threatresearch@infosec.exchange on Mastadon for up-to-the-minute news about all things malicious.

Read Similar Articles

MAY 24, 2021

What to expect when you've been hit with Avaddon...

MAY 19, 2021

What's New in Sophos EDR 4.0

MAY 19, 2021

Sophos XDR: Driven by data

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Subscribe to get the latest updates in your inbox.

name@email.com

Which categories are you interested in?

- [ ] Products and Services
- [ ] Threat Research
- [ ] Security Operations
- [ ] AI Research
- [ ] #SophosLife

Subscribe