Microsoft

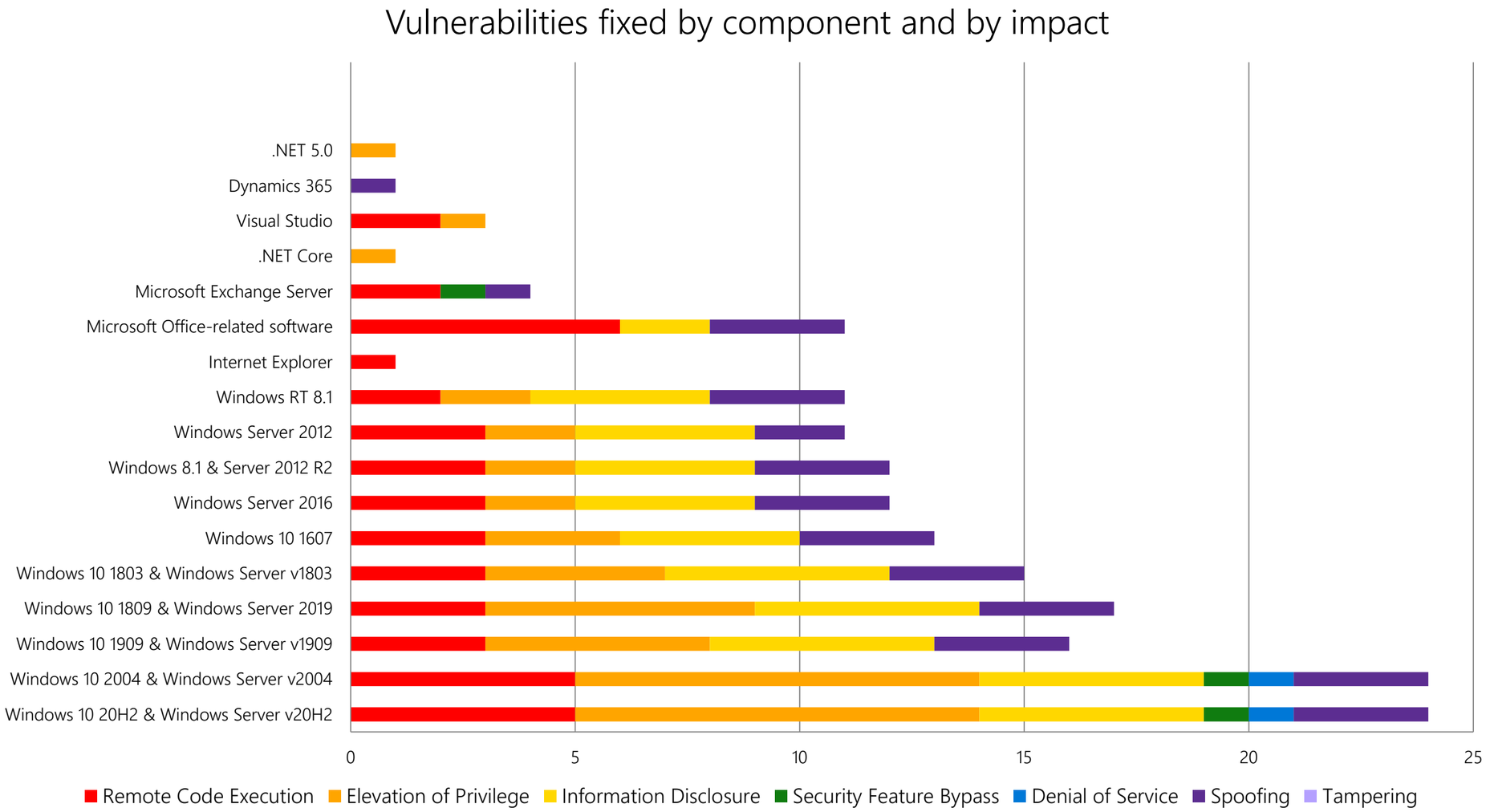
Microsoft Security Release

May 11, 2021

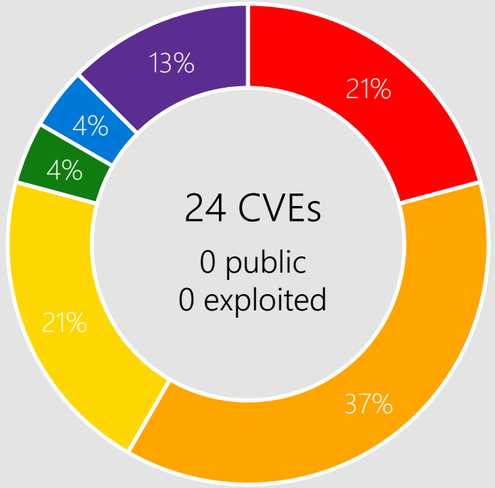
Agenda

- Security Updates
- Product Support Lifecyle
- Other resources related to the release

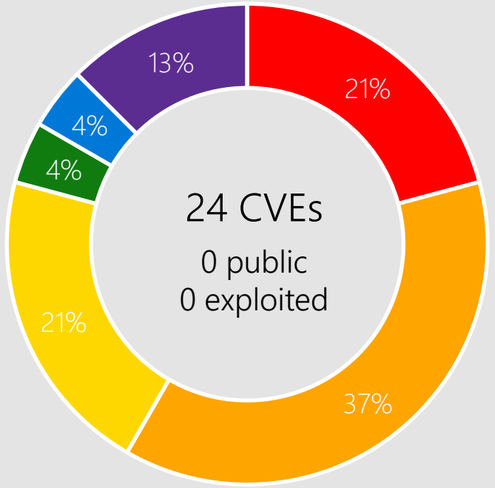
Monthly Security Release Overview - May 2021



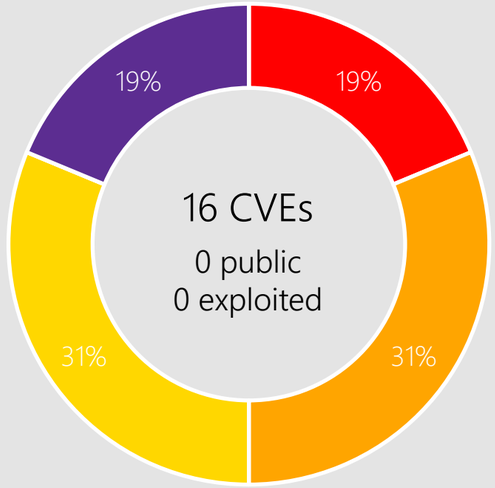
Windows 10



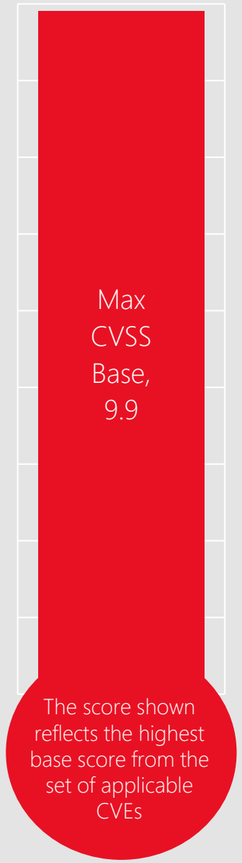
Windows 10 20H2 & Windows Server v20H2



Windows 10 2004 & Windows Server v2004



Windows 10 1909 & Windows Server v1909



Remote Code Execution | Elevation of Privilege | Information Disclosure | Security Feature Bypass | Denial of Service | Spoofing | Tampering

Affected Components:

Bluetooth Driver
Container Manager Service
CSC Service
Desktop Bridge
Graphics Component
HTTP Protocol Stack
Hyper-V
Infrared Data Association (IrDA)
Media Foundation Core
OLE Automation
Projected File System FS Filter Driver
RDP
SMB Client
SSDP Service
Jet Red Database Engine and Access Connectivity Engine

CVE-2021-31166 HTTP

Impact, Severity, Disclosure

Remote Code Execution| Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 9.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Windows 10
Server, version 2004
Server, version 20H2

CVE-2021-28476 Hyper-V

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 9.9 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

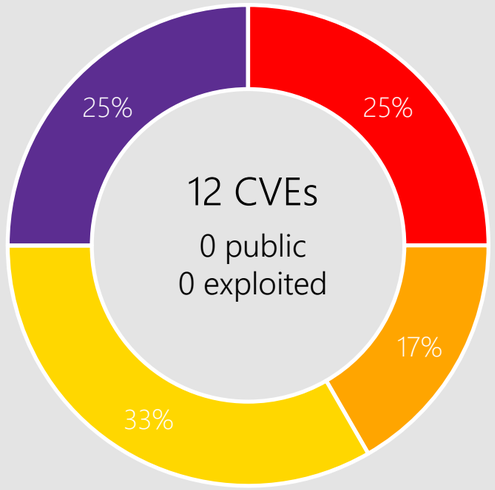
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

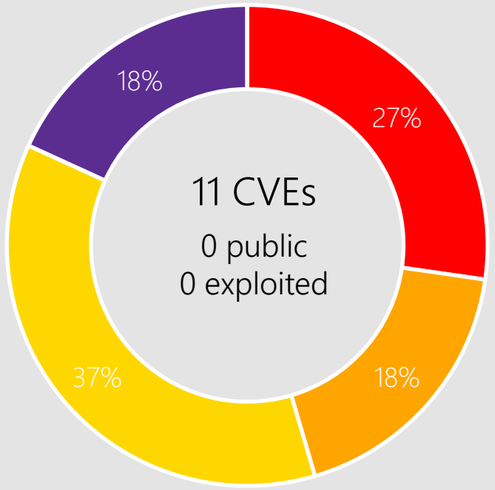
Affected Software

Server, version 20H2
Server, version 2004
Server, version 1909
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

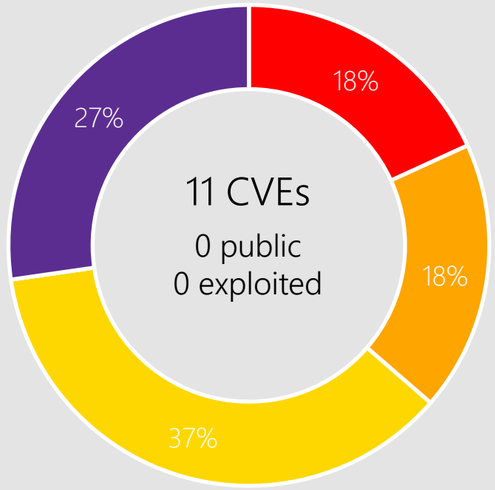
Windows 8.1, Server 2012 R2, and Server 2012



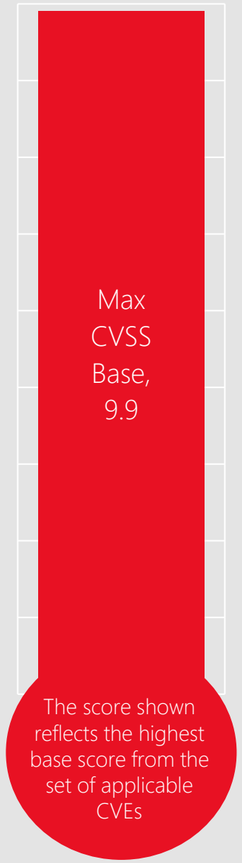
Windows 8.1 & Server 2012 R2



Windows Server 2012



Windows RT 8.1



Remote Code Execution Elevation of Privilege Information Disclosure Security Feature Bypass Denial of Service Spoofing Tampering

Affected Components:

Bluetooth Driver
CSC Service
Graphics Component

Hyper-V
Infrared Data Association (IrDA)

OLE Automation
Remote Desktop Protocol (RDP)
SSDP Service

Jet Red Database Engine and Access Connectivity Engine

CVE-2021-31194 OLE Automation

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Server, version 20H2
Server, version 2004
Server, version 1909
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

CVE-2021-26419 Scripting Engine

Impact, Severity, Disclosure

Remote Code Execution | Critical | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.5 | Attack Vector: Network | Attack Complexity: High | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

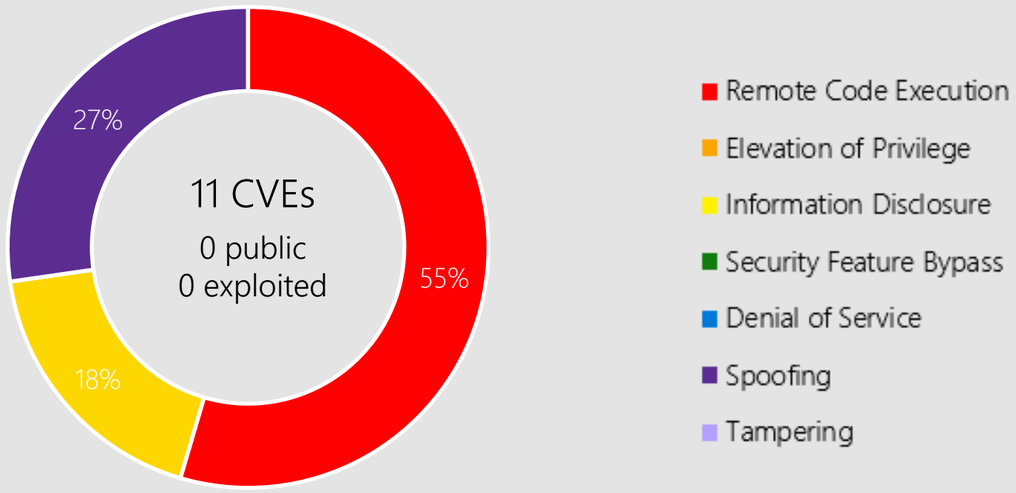
Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Internet Explorer 11

Microsoft Office



Microsoft Office-related software

Products:

Office 2013/2016/2019
Word 2013/2016
Excel 2013/2016
SharePoint Server 2019
SharePoint Enterprise Server 2016
365 Apps Enterprise
Lync Server 2013 CU10
Office 2019 for Mac
Office Online Server
Office Web Apps Server 2013
SharePoint Foundation 2013
Skype Business Server 2015 CU11
Skype Business Server 2019 CU5

CVE-2021-26422 Skype for Business and Lync

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.2 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: High | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Skype for Business Server 2015 CU11
Skype for Business Server 2019 CU5
Lync Server 2013 CU10

CVE-2021-28455 ACE and Jet Red DB Engine

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Recommended Actions

Disable ad-hoc queries in JET and ACE (Access Connectivity Engine).
See KB5002984: Configuring Jet Red Database Engine and Access Connectivity Engine to block access to remote databases
MSRC vulnerability entry https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28455

Affected Software

Windows Server 2012 R2
Windows Server 2012
Windows RT 8.1
Windows Server 2016
Windows 10
Server, version 20H2
Server, version 2004
Server, version 1909
Windows Server 2019
Office 2013/2016/2019
365 Apps for Enterprise

CVE-2021-28474 SharePoint Server

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

SharePoint Foundation 2013
SharePoint Server 2019
SharePoint Enterprise Server 2016

CVE-2021-31175 Office

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Excel 2013
Office 2016
Office Web Apps Server 2013
Office 2013
Office Online Server
Office 2019
Excel 2016
365 Apps Enterprise

CVE-2021-31180 Office Graphics

Impact, Severity, Disclosure

Remote Code Execution | Important | Privately disclosed | No known exploits in the wild

CVSSScoreMetrics

Base CVSS Score: 7.8 | Attack Vector: Local | Attack Complexity: Low | Privileges Required: None | User Interaction: Required

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Affected Software

Office 2013
Word 2013
Word 2016
Office 2019
365 Apps Enterprise

Other Products

Dynamics 365

CVE-2021-28461 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.1
Attack Vector: Adjacent
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: Dynamics 365 Finance and Operations

Other Products

Exchange Server

CVE-2021-31195 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2016 Cumulative Update 20, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8

CVE-2021-31198 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 7.8
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20

Other Products

Exchange Server

CVE-2021-31207 | Moderate | Security Feature Bypass | Public: Yes | Exploited: No

CVSS Base Score 6.6
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2016 Cumulative Update 20, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9

CVE-2021-31209 | Important | Spoofing | Public: No | Exploited: No

CVSS Base Score 6.5
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None
Products: Exchange Server 2016 Cumulative Update 19, Exchange Server 2019 Cumulative Update 8, Exchange Server 2013 Cumulative Update 23, Exchange Server 2019 Cumulative Update 9, Exchange Server 2016 Cumulative Update 20

Other Products

.NET 5.0

CVE-2021-31204 | Important | Elevation of Privilege | Public: Yes | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET Core 3.1, Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0

Other Products

.NET Core

CVE-2021-31204 | Important | Elevation of Privilege | Public: Yes | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET Core 3.1, Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0

Other Products

Visual Studio

CVE-2021-27068 | Important | Remote Code Execution | Public: No | Exploited: No

CVSS Base Score 8.8
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None
Products: Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)

CVE-2021-31204 | Important | Elevation of Privilege | Public: Yes | Exploited: No

CVSS Base Score 7.3
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
User Interaction: Required
Products: .NET Core 3.1, Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Visual Studio 2019 version 16.7 (includes 16.0 – 16.6), Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), .NET 5.0

Other Products

Developer Tools

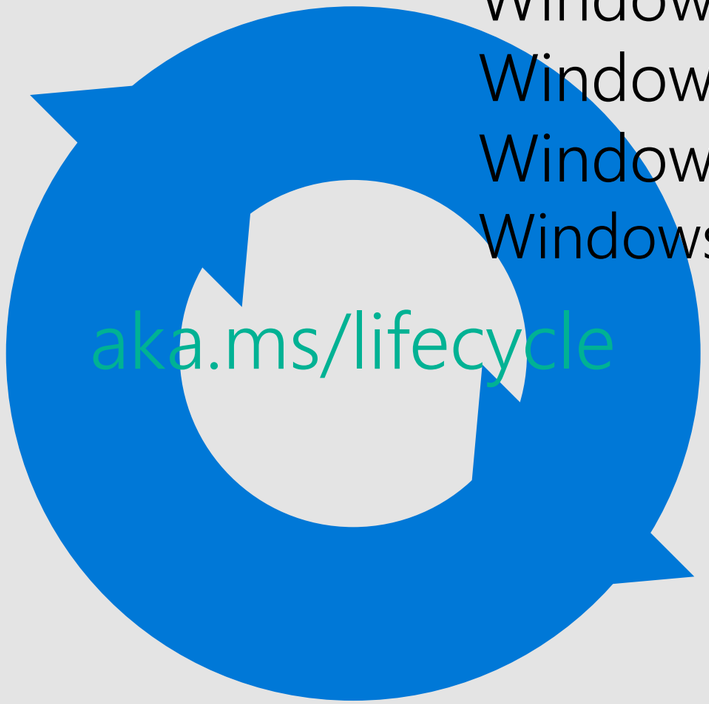
CVE-2021-31200 - common_utils.py
CVE-2021-31214 and CVE-2021-31211 - VS Code
CVE-2021-31213 – VS Code Remote Containers Extension

Product Lifecycle Update

No fixed lifecycle policy products reaching end of support in May

Windows 10 Semi-Annual Channel end of service

Windows 10 1803 Ent, Education
Windows 10 1809 Ent, Education
Windows 10 1909 Home, Pro, Pro Education
Windows Server, version 1909



Lifecycle changes to end of support and servicing dates

Windows Servicing Stack Updates

Product	SSU Package	Date Released
Windows 8.1/Server 2012 R2	5001403	April 2021
Windows Server 2012	5001401	April 2021
Windows 10 16076/Server 2016	5001402	April 2021
Windows 10 1803	5001400	April 2021
Windows 10 1809/Server 2019	5003244	May 2021
Windows 10 1909/Windows Server, version 1909	5003243	May 2021
Windows 10 2004/Windows Server, version 2004	Inc in monthly update	N/A
Windows 10 20H2/Windows Server, version 20H2	Inc in monthly update	N/A

Simplifying on-premises deployment of servicing stack updates - Microsoft Tech Community

Deploy Windows SSUs and LCUs together with one cumulative update - Microsoft Tech Community

Microsoft

Questions?

Appendix

CVE	Public	Exploited	Product
CVE-2020-24588	No	No	Wireless Networking
CVE-2020-24587	No	No	Wireless Networking
CVE-2020-26144	No	No	Wireless Networking
CVE-2021-28479	No	No	CSC Service
CVE-2021-31165	No	No	Container Manager Service
CVE-2021-31167	No	No	Container Manager Service
CVE-2021-31168	No	No	Container Manager Service
CVE-2021-31169	No	No	Container Manager Service
CVE-2021-31170	No	No	Graphics Component
CVE-2021-31180	No	No	Office Graphics
CVE-2021-31184	No	No	Infrared Data Association (IrDA)
CVE-2021-31185	No	No	Desktop Bridge
CVE-2021-31186	No	No	Remote Desktop Protocol (RDP)
CVE-2021-31187	No	No	WalletService

CVE	Public	Exploited	Product
CVE-2021-31188	No	No	Graphics Component
CVE-2021-31190	No	No	Container Isolation FS Filter Driver
CVE-2021-31191	No	No	Projected File System FS Filter Driver
CVE-2021-31192	No	No	Media Foundation Core
CVE-2021-31193	No	No	SSDP Service
CVE-2021-31194	No	No	OLE Automation
CVE-2021-31205	No	No	SMB Client
CVE-2021-31208	No	No	Container Manager Service
CVE-2021-28465	No	No	Web Media Extensions
CVE-2021-26419	No	No	Scripting Engine
CVE-2021-28455	No	No	Jet Red Database Engine and Access Connectivity Engine
CVE-2021-31171	No	No	SharePoint
CVE-2021-31172	No	No	SharePoint
CVE-2021-31173	No	No	SharePoint Server

CVE	Public	Exploited	Product
CVE-2021-31174	No	No	Excel
CVE-2021-31175	No	No	Office
CVE-2021-31176	No	No	Office
CVE-2021-31177	No	No	Office
CVE-2021-31178	No	No	Office
CVE-2021-31179	No	No	Office
CVE-2021-31181	No	No	SharePoint
CVE-2021-26421	No	No	Skype for Business and Lync
CVE-2021-26422	No	No	Skype for Business and Lync
CVE-2021-28474	No	No	SharePoint Server
CVE-2021-28478	No	No	SharePoint
CVE-2021-26418	No	No	SharePoint
CVE-2021-31936	No	No	Accessibility Insights for Web
CVE-2021-27068	No	No	Visual Studio

CVE	Public	Exploited	Product
CVE-2021-28461	No	No	Dynamics Finance and Operations Cross-site Scripting
CVE-2021-31166	No	No	HTTP Protocol Stack
CVE-2021-31182	No	No	Bluetooth Driver
CVE-2021-31195	No	No	Exchange Server
CVE-2021-31198	No	No	Exchange Server
CVE-2021-31204	Yes	No	.NET Core and Visual Studio
CVE-2021-31207	Yes	No	Exchange Server
CVE-2021-31209	No	No	Exchange Server
CVE-2021-31211	No	No	Visual Studio Code Remote Development Extension
CVE-2021-31213	No	No	Visual Studio Code Remote Development Extension
CVE-2021-31214	No	No	Visual Studio Code
CVE-2021-28476	No	No	Hyper-V
CVE-2021-31200	Yes	No	Common Utilities