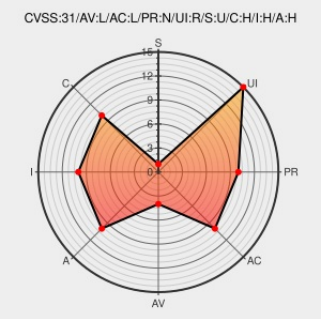
CVE-2020-1147

Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-1147

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of .net Core from Microsoft contain the following vulnerability:

A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.

CVE-2020-1147 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SharePoint DataSet / DataTable Deserialization ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158694/SharePoint-DataSet-DataTable-Deserialization.html
Microsoft SharePoint Server 2019 Remote	packetstormsecurity.com	MISC packetstormsecurity.com/files/163644/Microsoft-

Microsoft SharePoint Server 2019 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158876/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html
Microsoft SharePoint Server 2019 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158876/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html
Microsoft SharePoint Server 2019 Remote Code Execution - Exploitalert	www.exploitalert.com text/x-python	MISC www.exploitalert.com/view-details.html?id=35992
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Core	2.1	All	All	All
Application	Microsoft	.net Core	3.1	All	All	All
Application	Microsoft	.net Core	2.1	All	All	All
Application	Microsoft	.net Core	3.1	All	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.5.2	All	All	All
Application	Microsoft	.net Framework	4.6	All	All	All
Application	Microsoft	.net Framework	4.6.1	All	All	All
Application	Microsoft	.net Framework	4.6.2	All	All	All
Application	Microsoft	.net Framework	4.7	All	All	All
Application	Microsoft	.net Framework	4.7.1	All	All	All
Application	Microsoft	.net Framework	4.7.2	All	All	All
Application	Microsoft	.net Framework	4.8	All	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.5.2	All	All	All

Application	Microsoft	.net Framework	4.6	All	All	All
Application	Microsoft	.net Framework	4.6.1	All	All	All
Application	Microsoft	.net Framework	4.6.2	All	All	All
Application	Microsoft	.net Framework	4.7	All	All	All
Application	Microsoft	.net Framework	4.7.1	All	All	All
Application	Microsoft	.net Framework	4.7.2	All	All	All
Application	Microsoft	.net Framework	4.8	All	All	All
Application	Microsoft	Sharepoint Enterprise Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Enterprise Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Server	2010	sp2	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All
Application	Microsoft	Sharepoint Server	2010	sp2	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All
Application	Microsoft	Visual Studio 2017	All	All	All	All
Application	Microsoft	Visual Studio 2019	All	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All

Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All

Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

cpe:2.3:a:microsoft:.net_core:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_core:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_core:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_core:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:2.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.5:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.8:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:2.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.5:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.8:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2013:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2016:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2013:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2016:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_server:2010:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_server:2010:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_2017:*:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_2019:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1709:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1803:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1709:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1803:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:-:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:-:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:

cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1803:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1903:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1909:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1803:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1903:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:1909:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2020-1147.... twitter.com/i/web/status/1…	2021-11-19 02:02:01
@ipssignatures	I know 6 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-1147. ipssignatures.appspot.com/?cve=CVE-2020-… #Sd5jutrevzbwds	2021-11-19 02:02:01
@OPOSEC	Remote Code Execution Against SharePoint Server Abusing DataSet (CVE-2020-1147). bit.ly/2ZQHYq2 (+) #Security #336 (2020)	2022-02-10 08:00:02
@RemotelyAlerts	Severity: ?? | A remote code execution vulnerability ex... | CVE-2020-1147 | Link for more: alerts.remotelyrmm.com/CVE-2020-1147	2022-04-01 22:29:50
/r/sysadmin	Vulnerability found in Microsoft Visual Studio Tools for Applications 2017 - update?	2021-09-15 17:59:30
/r/SCCM	Defender Vulnerability CVEs & Patching	2022-05-06 07:29:16

← Previous ID

Next ID→