



CVE-2020-16952

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:49 PM UTC

CVE-2020-16952

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Sharepoint Enterprise Server](#) from [Microsoft](#) contain the following vulnerability:

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16951.

CVE-2020-16952 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Microsoft - Microsoft SharePoint Enterprise Server 2016** version

Affected Vendor/Software: **Microsoft - Microsoft SharePoint Server 2019** version

Affected Vendor/Software: **Microsoft - Microsoft SharePoint Foundation 2013 Service Pack 1** version

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
Microsoft SharePoint SSI / ViewState Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/159612/Microsoft-SharePoint-SSI-ViewState-Remote-Code-Execution.html
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	 MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16952

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Foundation	2013	sp1	All	All
Application	Microsoft	Sharepoint Foundation	2013	sp1	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All

```
cpe:2.3:a:microsoft:sharepoint enterprise server:2016:*:*:*:*.*.*
```

```
cpe:2.3:a:microsoft:sharepoint enterprise server:2016:*:*:*:*.*.*
```

cpe:2.3:a:microsoft:sharepoint foundation:2013:sp1:*:*:*:*:*:

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

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

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)