



CVE-2020-1466

Published on: 08/17/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

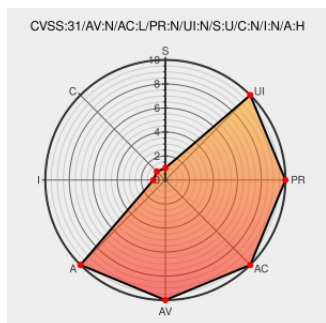
CVE-2020-1466

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Windows Server 2012](#) from [Microsoft](#) contain the following vulnerability:

A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability'.

CVE-2020-1466 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

NONE

NONE

HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

Patch

Vendor Advisory

portal.msrc.microsoft.com

MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1466

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
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	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
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:-:~::~~::~~::~~::~~::~~::~~::						
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

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)