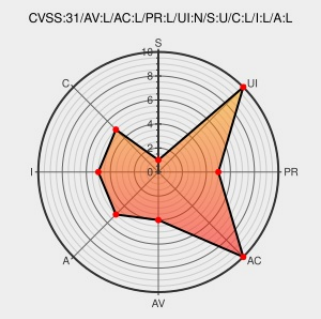
CVE-2019-9510

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:07 PM UTC

CVE-2019-9510 - advisory for VU#576688

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



Certain versions of Windows 10 from Microsoft contain the following vulnerability:

A vulnerability in Microsoft Windows 10 1803 and Windows Server 2019 and later systems can allow authenticated RDP-connected clients to gain access to user sessions without needing to interact with the Windows lock screen. Should a network anomaly trigger a temporary RDP disconnect, Automatic Reconnection of the RDP session will be restored to an unlocked state, regardless of how the remote system was left. By interrupting network connectivity of a system, an attacker with access to a system being used as a Windows RDP client can gain access to a connected remote system, regardless of whether or not the remote system was locked. This issue affects Microsoft Windows 10, version 1803 and later, and Microsoft Windows Server 2019, version 2019 and later.

CVE-2019-9510 has been assigned by cert@cert.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Microsoft** - **Windows 10 or newer system using RDP** version **>= 1803**

Affected Vendor/Software: **Microsoft** - **Windows Server** version **>= 2019**

Vulnerability Patch/Work Around

Disable RDP automatic reconnection on RDP servers. Disconnect RDP sessions instead of locking them.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Configure Network Level Authentication for Remote Desktop Services Connections | Microsoft Docs	Patch Vendor Advisory docs.microsoft.com text/html	MISC docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)
[MS-RDPBCGR]: Automatic Reconnection | Microsoft Docs	Patch Vendor Advisory docs.microsoft.com text/html	MISC docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/e729948a-3f4e-4568-9aef-d355e30b5389
RDS 2019 (but probably other versions as well): locked RDP session logs in after session reconnect	Patch Vendor Advisory social.technet.microsoft.com text/html	MISC social.technet.microsoft.com/Forums/windowsserver/en-US/1fd171de-a1b5-4721-86bf-082e4a375049/rds-2019-but-probably-other-versions-as-well-locked-rdp-session-logs-in-after-session-reconnect
VU#576688 - Microsoft Windows RDP can bypass the Windows lock screen	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#576688

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 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1803	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_10:1803:*:*:*:*:*:*:*:

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

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

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

Discovery Credit

Thanks to Joe Tammariello of the SEI for reporting this vulnerability.

← Previous ID

Next ID→