



CVE-2017-8673

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-8673
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-08 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 10 1703 allows an attacker to connect to a target and execute arbitrary code with SYSTEM privileges.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All

References

Reference	Source
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8673	CONFIRM
Windows Remote Desktop Protocol (RDP) Lets Remote Users Cause the Target Service to Stop Responding - SecurityTracker	SECTRACK
Microsoft Windows Remote Desktop Protocol CVE-2017-8673 Denial of Service Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report