Microsoft MSRC | Security Updates Acknowledgements Sign in

MSRC > Customer Guidance > Security Update Guide > Advisories > CVE 2019 0708

Remote Desktop Services Remote Code Execution Vulnerability

On this page

CVE-2019-0708
Security Vulnerability

Subscribe RSS PowerShell { } API

Released: May 14, 2019

Assigning CNA: Microsoft

CVE-2019-0708

Executive Summary

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

Exploitability

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly disclosed
No
Exploited
No
Exploitability assessment
N/A

Mitigations

The following mitigation may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave Remote Desktop Services disabled:

1. Disable Remote Desktop Services if they are not required.

If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

Workarounds

The following workarounds may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave these workarounds in place:

1. Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2