Microsoft

 Report an issue~

All Microsoft~

Sign in (/en-us/signin)

Security Update Guide (/en-us/security-guidance) > Details

Customer guidance~

United States (English)

# CVE-2017-8714 | Remote Desktop Virtual Host Remote Code Execution Vulnerability

Security Vulnerability

Published: 09/12/2017 | Last Updated : 09/12/2017

MITRE CVE-2017-8714 (https://cve.mitre.org/cgi-bin/cvename.cgi?name\_eVte2019~8714)

A remote code execution vulnerability exists in the VM Host Agent Service of Remote Desktop Virtual Host role when it fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could issue a specially crafted certificate on the guest operating system that could cause the VM host agent service on the host operating system to execute arbitrary code. The Remote Desktop Virtual Host role is not enabled by default.

Engage~

An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.

The security update addresses the vulnerability by correcting how VM host agent service validates guest operating system user input.

#### On this page

**Executive Summary** 

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EN)

**Exploitability Assessment** 

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EA)

Security Updates

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EGB)

Mitigations

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EMGAC)

Workarounds

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EUGAC)

FAQ

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EKIAC)

Acknowledgements

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EWIAC)

Disclaimer

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0ECJAC)

Revisions

(https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8714#ID0EHJAC)

## **Exploitability Assessment**

The following table provides an exploitability assessment (https://technet.microsoft.com/en-us/security/cc998259.aspx) for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable

Security Updates

CVSS Score

## Security Updates

To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle (https://support.microsoft.com/en-us/lifecycle).

Product ▲	Platform	Article	Download	Impact	Severity	Superse
Windows 10 Version 1607 for x64-based Systems		4038782 (https://support.microsoft.com/help/4038782)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038782)	Remote Code Execution	Important	4034658

Product A	Platform	Article	Download	Impact	Severity	Superse
Windows 8.1 for x64- based systems		4038792 (https://support.microsoft.com/help/4038792)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038792)	Remote Code Execution	Important	4034681
		4038793 (https://support.microsoft.com/help/4038793)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038793)			
Windows Server 2012		4038799 (https://support.microsoft.com/help/4038799)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038799)	Remote Code Execution	Important	4034665
		4038786 (https://support.microsoft.com/help/4038786)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038786)			
Windows Server 2012 (Server Core installation)		4038799 (https://support.microsoft.com/help/4038799)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038799)	Remote Code Execution	Important	4034665
		4038786 (https://support.microsoft.com/help/4038786)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038786)			
Windows Server 2012 R2		4038792 (https://support.microsoft.com/help/4038792)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038792)	Remote Code Execution	Important	4034681
		4038793 (https://support.microsoft.com/help/4038793)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038793)			
Windows Server 2012 R2 (Server Core installation)		4038792 (https://support.microsoft.com/help/4038792)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038792)	Remote Code Execution	Important	4034681
		4038793 (https://support.microsoft.com/help/4038793)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038793)			
Windows Server 2016		4038782 (https://support.microsoft.com/help/4038782)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038782)	Remote Code Execution	Important	4034658
Windows Server 2016 (Server Core installation)		4038782 (https://support.microsoft.com/help/4038782)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx? q=KB4038782)	Remote Code Execution	Important	4034658

## Mitigations

Microsoft has not identified any mitigating factors (https://technet.microsoft.com/library/security/dn848375.aspx#Mitigation) for this vulnerability.

## Workarounds

Microsoft has not identified any workarounds (https://technet.microsoft.com/library/security/dn848375.aspx#Workaround) for this vulnerability.

## Acknowledgements

Jared S. Candelaria (https://twitter.com/jsc29a)

 $See \ a cknowledgements \ (https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments) \ for \ more \ information.$ 

## Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

## Revisions

Version	Date	Description
1.0	09/12/2017	Information published.
1.1	09/12/2017	Removed Windows 10 for x64-based Systems as affected by CVE-2017-8714. This is an informational change only.

What's new	Microsoft Store	Education	Enterprise	Developer	Company
Surface Pro 6 (https://www.microsoft.com/en -us/p/surface-pro- 6/8ZCNC665SLQ5)	Account profile (https://account.microsoft.co m/)	Microsoft in education (https://www.microsoft.com/ en-us/education)	Azure (https://azure.microsoft.com/) AppSource	Microsoft Visual Studio (https://visualstudio.microsof t.com/)	Careers (https://careers.microsoft.co m/)
Surface Laptop 2 (https://www.microsoft.com/en -us/p/surface-laptop-	Download Center (https://www.microsoft.com/ en-us/download)	Office for students (https://www.microsoft.com/ en- us/education/products/office	(https://go.microsoft.com/fwlin k/?LinkID=808093)	Windows Dev Center (https://developer.microsoft. com/en-us/windows)	About Microsoft (https://www.microsoft.com/ en-us/about)
2/8XQJKK3DD91B)	Microsoft Store support (https://go.microsoft.com/fwl	/default.aspx)  Office 365 for schools	(https://www.microsoft.com/en -us/enterprise/automotive)	Developer Network (https://msdn.microsoft.com/	Company news (https://news.microsoft.com/
(https://www.microsoft.com/en -us/p/surface-	ink/p/? LinkID=824761&clcid=0x409 )	(https://products.office.com/ en-us/academic/compare-	Government (https://www.microsoft.com/en	en-us) TechNet	Privacy at Microsoft
go/8v9dp4lnknsz) Xbox One X	Returns (https://go.microsoft.com/fwl	office-365-education-plans)  Deals for students & parents	-us/enterprise/government)	(https://technet.microsoft.co m/en-us)	(https://privacy.microsoft.co m/en-us)
(https://www.xbox.com/en- us/xbox-one-x)	ink/p/? LinkID=824764&clcid=0x409	(https://www.microsoft.com/ en-us/store/b/education? icid=CNavfooter_Studentsan	(https://www.microsoft.com/en -us/enterprise/health)	Microsoft developer program (https://developer.microsoft.	Investors (https://www.microsoft.com/i nvestor/default.aspx)
Xbox One S (https://www.xbox.com/en- us/xbox-one-s?xr=shellnav)	Order tracking (https://account.microsoft.co	deducation)  Microsoft Azure in education	Manufacturing (https://www.microsoft.com/en -us/enterprise/manufacturing)	com/en-us/store/register) Channel 9	Diversity and inclusion (https://www.microsoft.com/
VR & mixed reality	m/orders)	(https://azure.microsoft.com/ en-	Financial services	(https://channel9.msdn.com/ )	en-us/diversity/)
(https://www.microsoft.com/en -us/store/b/virtualreality)	Store locations (https://www.microsoft.com/ en-us/store/locations/find-a-	us/community/education/)	(https://www.microsoft.com/en - us/enterprise/finance/banking-	Office Dev Center (https://developer.microsoft.	Accessibility (https://www.microsoft.com/ en-us/accessibility)
Windows 10 apps (https://www.microsoft.com/en -us/windows/windows-10-	store?icid=en-us_UF_FAS)  Buy online, pick up in store		capital-markets)	com/en-us/office) Microsoft Garage	Security (https://www.microsoft.com/
apps)	(https://www.microsoft.com/ en-us/store/b/buy-online-		(https://www.microsoft.com/en -us/enterprise/retail-consumer-	(https://www.microsoft.com/ en-us/garage/)	en-us/security/default.aspx)
Office apps	pick-up-in-store?		goods)		

(https://store.office.com/en-

us/appshome.aspx?)

English (United States)(https://www.microsoft.com/en-us/locale.aspx)

icid=uhf\_footer\_bopuis)

Sitemap (https://www.microsoft.com/en-us/sitemap1.aspx)

Contact Microsoft (https://support.microsoft.com/en-us/contactus)

Privacy & cookies (https://go.microsoft.com/fwlink/?Linkld=521839) Terms of use (https://go.microsoft.com/fwlink/?LinklD=206977) Trademarks (https://www.microsoft.com/trademarks)

Safety & eco (https://www.microsoft.com/en-us/devices/safety-and-eco ) About our ads (https://choice.microsoft.com) © Microsoft 2019