CVE-2017-11780 | Windows SMB 远程代码执行漏洞

安全漏洞

发布时间: 2017-10-10
MITRE CVE-2017-11780 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11780)

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.

To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

本页内容

利用指数评估

下表为此漏洞提供初始发布时的利用指数评估。

公开披露	已受攻击	最新软件版本	较旧软件版本	拒绝服务
否	否	1 - 更有可能被利用	1 - 更有可能被利用	不适用

受影响的产品 | CVSS 分数

受影响的产品

下列软件版本会受到影响。未列出的版本的支持生命周期已结束或不受影响。若要确定你的软件版本的支持生命周期，请参阅 Microsoft 支持生命周期 (https://support.microsoft.com/en-us/lifecycle)。

产品 ▲	平台	文章	下载	影响	严重性	取代
Windows 10 for 32-bit Systems		4042895 (https://support.microsoft.com/help/4042895)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4042895)	远程执行代码	重要	4038781
Windows 10 for x64-based Systems		4042895 (https://support.microsoft.com/help/4042895)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4042895)	远程执行代码	重要	4038781
Windows 10 Version 1511 for 32-bit Systems		4041689 (https://support.microsoft.com/help/4041689)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041689)	远程执行代码	重要	4038783
Windows 10 Version 1511 for x64-based Systems		4041689 (https://support.microsoft.com/help/4041689)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041689)	远程执行代码	重要	4038783
Windows 10 Version 1607 for 32-bit Systems		4041691 (https://support.microsoft.com/help/4041691)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691)	远程执行代码	重要	4038782

产品 ▲	平台	文章	下载	影响	严重性	取代
Windows 10 Version 1607 for x64-based Systems		4041691 (https://support.microsoft.com/help/4041691)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691)	远程执行代码	重要	4038782
Windows 10 Version 1703 for 32-bit Systems		4041676 (https://support.microsoft.com/help/4041676)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041676)	远程执行代码	重要	4038788
Windows 10 Version 1703 for x64-based Systems		4041676 (https://support.microsoft.com/help/4041676)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041676)	远程执行代码	重要	4038788
Windows 7 for 32-bit Systems Service Pack 1		4041681 (https://support.microsoft.com/help/4041681)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681)	远程执行代码	重要	4038777
		4041678 (https://support.microsoft.com/help/4041678)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678)			
Windows 7 for x64-based Systems Service Pack 1		4041681 (https://support.microsoft.com/help/4041681)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681)	远程执行代码	重要	4038777
		4041678 (https://support.microsoft.com/help/4041678)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678)			
Windows 8.1 for 32-bit systems		4041693 (https://support.microsoft.com/help/4041693)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693)	远程执行代码	重要	4038792
		4041687 (https://support.microsoft.com/help/4041687)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041687)			

产品 ▲	平台	文章	下载	影响	严重性	取代
Windows 8.1 for x64-based systems		4041693 (https://support.microsoft.com/help/4041693)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693)	远程执行代码	重要	4038792
		4041687 (https://support.microsoft.com/help/4041687)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041687)			
Windows RT 8.1		4041693 (https://support.microsoft.com/help/4041693)	Monthly Rollup	远程执行代码	重要	4038792
Windows Server 2008 for 32-bit Systems Service Pack 2		4041995 (https://support.microsoft.com/help/4041995)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995)	远程执行代码	重要	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)		4041995 (https://support.microsoft.com/help/4041995)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995)	远程执行代码	重要	
Windows Server 2008 for Itanium-Based Systems Service Pack 2		4041995 (https://support.microsoft.com/help/4041995)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995)	远程执行代码	重要	
Windows Server 2008 for x64-based Systems Service Pack 2		4041995 (https://support.microsoft.com/help/4041995)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995)	远程执行代码	重要	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)		4041995 (https://support.microsoft.com/help/4041995)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995)	远程执行代码	重要	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1		4041681 (https://support.microsoft.com/help/4041681)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681)	远程执行代码	重要	4038777

产品 ▲	平台	文章	下载	影响	严重性	取代
		4041678 (https://support.microsoft.com/help/4041678)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678)			
Windows Server 2008 R2 for x64-based Systems Service Pack 1		4041681 (https://support.microsoft.com/help/4041681)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681)	远程执行代码	重要	4038777
		4041678 (https://support.microsoft.com/help/4041678)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678)			
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)		4041681 (https://support.microsoft.com/help/4041681)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681)	远程执行代码	重要	4038777
		4041678 (https://support.microsoft.com/help/4041678)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678)			
Windows Server 2012		4041690 (https://support.microsoft.com/help/4041690)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041690)	远程执行代码	重要	4038799
		4041679 (https://support.microsoft.com/help/4041679)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041679)			
Windows Server 2012 (Server Core installation)		4041690 (https://support.microsoft.com/help/4041690)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041690)	远程执行代码	重要	4038799
		4041679 (https://support.microsoft.com/help/4041679)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041679)			

产品 ▲	平台	文章	下载	影响	严重性	取代
Windows Server 2012 R2		4041693 (https://support.microsoft.com/help/4041693)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693)	远程执行代码	重要	4038792
		4041687 (https://support.microsoft.com/help/4041687)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041687)			
Windows Server 2012 R2 (Server Core installation)		4041693 (https://support.microsoft.com/help/4041693)	Monthly Rollup (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693)	远程执行代码	重要	4038792
		4041687 (https://support.microsoft.com/help/4041687)	Security Only (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041687)			
Windows Server 2016		4041691 (https://support.microsoft.com/help/4041691)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691)	远程执行代码	重要	4038782
Windows Server 2016 (Server Core installation)		4041691 (https://support.microsoft.com/help/4041691)	Security Update (https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691)	远程执行代码	重要	4038782

缓解

The file sharing protocol SMB is often disabled on the perimeter firewall. This limits the potential attack vectors for this vulnerability. Please see 2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and) for more information.

变通方法

Microsoft 尚未对此漏洞确认任何变通办法 (https://technet.microsoft.com/library/security/dn848375.aspx#Workaround)。

鸣谢

Nicolas Joly of MSRC Vulnerabilities & Mitigations

有关详细信息，请参阅鸣谢 (https://portal.msrc.microsoft.com/zh-cn/security-guidance/acknowledgments)。

免责声明

修订

版本	日期	说明
1.0	2017-10-10	已发布的信息。