

Search vulnerability database

Q

Multiple vulnerabilities in Microsoft Windows SMB

Published: 2019-03-12 | Updated: 2019-05-08



Severity	<div><div></div>Medium</div>
Patch available	<div><div></div>YES</div>
Number of vulnerabilities	3
CVE ID	CVE-2019-0703 CVE-2019-0821 CVE-2019-0704
CWE ID	CWE-200
Exploitation vector	Local network
Public exploit	Vulnerability #1 is being exploited in the wild.
Vulnerable software	Windows Operating systems & Components / Operating system
	Windows Server Operating systems & Components / Operating system
Vendor	Microsoft

Security Advisory

UPDATED: 08.05.2019

Vulnerability #1 was updated to reflect latest information from Symantec. Severity of this bulletin was increased to Medium.

1) Information disclosure

Severity: Medium

CVSSv3: [3.4 \[CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C\]](#)

CVE-ID: CVE-2019-0703

CWE-ID: [CWE-200 - Information Exposure](#)

Exploit availability: Yes

Description

The vulnerability allows a remote authenticated attacker to gain access to potentially sensitive information.

The vulnerability exists due to the way that the Windows SMB Server handles certain requests. A remote authenticated user can gain unauthorized access to sensitive information on the system.

Note: this vulnerability has being exploited in the wild. The exploit code was detected in the Bemstour exploit tool in September 2018 and has being used by Buckeye (APT3) APT group.

Mitigation

Install updates from vendor's website.

Vulnerable software versions

Windows: 7, 8.1, 10, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, RT 8.1

Windows Server: 1709, 1803, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019

CPE

- [cpe:/a:microsoft:windows:8.1:](#)
- [cpe:/a:microsoft:windows:7:](#)
- [cpe:/a:microsoft:windows:10:](#)
- [cpe:/a:microsoft:windows:RT 8.1:](#)
- [cpe:/a:microsoft:windows:10 1607:](#)
- [cpe:/a:microsoft:windows:10 1703:](#)
- [cpe:/a:microsoft:windows:10 1709:](#)
- [cpe:/a:microsoft:windows:10 1803:](#)
- [cpe:/a:microsoft:windows:10 1809:](#)
- [cpe:/a:microsoft:windows_server:2012:](#)
- [cpe:/a:microsoft:windows_server:2012 R2:](#)
- [cpe:/a:microsoft:windows_server:2008:](#)
- [cpe:/a:microsoft:windows_server:2008 R2:](#)
- [cpe:/a:microsoft:windows_server:2016:](#)
- [cpe:/a:microsoft:windows_server:2019:](#)
- [cpe:/a:microsoft:windows_server:1709:](#)
- [cpe:/a:microsoft:windows_server:1803:](#)

External links

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703>

<https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit>

Q & A

Can this vulnerability be exploited remotely?

Yes. This vulnerability can be exploited by a remote authenticated user via the local network (LAN).

Is there known malware, which exploits this vulnerability?

Yes. This vulnerability is being exploited in the wild.

2) Information disclosure

Severity: Low

CVSSv3: [3.1 \[CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C\]](#)

CVE-ID: CVE-2019-0821

CWE-ID: [CWE-200 - Information Exposure](#)

Exploit availability: No

Description

The vulnerability allows a remote authenticated attacker to gain access to potentially sensitive information.

The vulnerability exists due to the way that the Windows SMB Server handles certain requests. A remote authenticated user can gain unauthorized access to sensitive information on the system.

Mitigation

Install updates from vendor's website.

Vulnerable software versions

Windows: 7, 8.1, 10, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, RT 8.1

Windows Server: 1709, 1803, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019

CPE

- [cpe:/a:microsoft:windows:8.1:](#)
- [cpe:/a:microsoft:windows:7:](#)
- [cpe:/a:microsoft:windows:10:](#)
- [cpe:/a:microsoft:windows:RT 8.1:](#)
- [cpe:/a:microsoft:windows:10 1607:](#)
- [cpe:/a:microsoft:windows:10 1703:](#)
- [cpe:/a:microsoft:windows:10 1709:](#)
- [cpe:/a:microsoft:windows:10 1803:](#)
- [cpe:/a:microsoft:windows:10 1809:](#)
- [cpe:/a:microsoft:windows_server:2012:](#)
- [cpe:/a:microsoft:windows_server:2012 R2:](#)
- [cpe:/a:microsoft:windows_server:2008:](#)

- [cpe:/a:microsoft:windows_server:2008 R2:](#)
- [cpe:/a:microsoft:windows_server:2016:](#)
- [cpe:/a:microsoft:windows_server:2019:](#)
- [cpe:/a:microsoft:windows_server:1709:](#)
- [cpe:/a:microsoft:windows_server:1803:](#)

External links

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821>

Q & A

Can this vulnerability be exploited remotely?

Yes. This vulnerability can be exploited by a remote authenticated user via the local network (LAN).

Is there known malware, which exploits this vulnerability?

No. We are not aware of malware exploiting this vulnerability.

3) Information disclosure

Severity: Low

CVSSv3: [3.1 \[CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/N/A/NF:U/RL:O/RC:C\]](#)

CVE-ID: CVE-2019-0704

CWE-ID: [CWE-200 - Information Exposure](#)

Exploit availability: No

Description

The vulnerability allows a remote authenticated attacker to gain access to potentially sensitive information.

The vulnerability exists due to the way that the Windows SMB Server handles certain requests. A remote authenticated user can gain unauthorized access to sensitive information on the system.

Mitigation

Install updates from vendor's website.

Vulnerable software versions

Windows: 7, 8.1, 10, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, RT 8.1

Windows Server: 1709, 1803, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019

CPE

- [cpe:/a:microsoft:windows:8.1:](#)
- [cpe:/a:microsoft:windows:7:](#)
- [cpe:/a:microsoft:windows:10:](#)
- [cpe:/a:microsoft:windows:RT 8.1:](#)
- [cpe:/a:microsoft:windows:10 1607:](#)
- [cpe:/a:microsoft:windows:10 1703:](#)
- [cpe:/a:microsoft:windows:10 1709:](#)
- [cpe:/a:microsoft:windows:10 1803:](#)
- [cpe:/a:microsoft:windows:10 1809:](#)
- [cpe:/a:microsoft:windows_server:2012:](#)
- [cpe:/a:microsoft:windows_server:2012 R2:](#)
- [cpe:/a:microsoft:windows_server:2008:](#)
- [cpe:/a:microsoft:windows_server:2008 R2:](#)
- [cpe:/a:microsoft:windows_server:2016:](#)
- [cpe:/a:microsoft:windows_server:2019:](#)
- [cpe:/a:microsoft:windows_server:1709:](#)
- [cpe:/a:microsoft:windows_server:1803:](#)

External links

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704>

Q & A

Can this vulnerability be exploited remotely?

Yes. This vulnerability can be exploited by a remote authenticated user via the local network (LAN).

Is there known malware, which exploits this vulnerability?

No. We are not aware of malware exploiting this vulnerability.

0 Comments

Sort by **Oldest** ▾



Add a comment...

Facebook Comments Plugin

Get in touch

+420 775 359 903

Stay Connected



Security Services

SaaS Vulnerability Scanner

Actionable & Personalized
Vulnerability Intelligence

On-Demand Security
Consulting

Pricing



IT-Consulting

On-Demand Consulting

IT Infrastructure Outsourcing
Services

Web Applications Support &
Deployment

Free Services

Free Online Vulnerability and
Port Scanner

SSL/TLS Security Test by
ImmunWeb

Web Server Security Test by
ImmunWeb

Blog

Microsoft rolls out Windows 10 KB4551762
update to address the critical SMBv3
vulnerability

Criminals are exploiting coronavirus scare to
infect computers with malware

Microsoft discloses a new wormable Win
SMBv3 CVE-2020-0796 flaw

Nation-state hackers compromise Microsoft
Exchange servers vulnerable to CVE-2020-0688

Critical PPP Daemon vulnerability puts most of
Linux systems at risk of remote attacks

[Read all articles →](#)



© 2020 Cybersecurity Help s.r.o.

[Contacts](#) | [Terms of use](#) | [Privacy Policy](#)