



TODAY'S TOP STORIES

FortiGuard SSH backdoor found in more Fortinet security appliances

FortiSwitch, FortiAnalyzer and FortiCache were also affected



By **Lucian Constantin** | Follow

IDG News Service | Jan 22, 2016 10:30 AM PT

Network security vendor Fortinet has identified an authentication issue that could give remote attackers administrative control over some of its products.

The issue, which was described as a FortiGuard SSH (Secure Shell) backdoor, was originally disclosed earlier this month by an anonymous researcher, who also published exploit code for it.

Last week, Fortinet said that the problem was not an intentional backdoor, but the result of a management feature which relied on an undocumented account with a hard-coded password. Additionally the company noted that the issue was fixed in FortiOS back in July 2014, after being identified as a security risk by the company's own product security team.

Compare: HP ArcSight vs Splunk

FortiOS is the operating system that runs on Fortinet's FortiGuard network firewall appliances. The versions patched in 2014 were FortiOS 4.3.17 and FortiOS 5.0.8, while the newer 5.2 and 5.4 branches have never been affected.

However, after its statement last week, the company began investigating if the same issue also exists in other products and found that some versions of FortiSwitch, FortiAnalyzer and FortiCache are also affected.


"These versions have the same management authentication issue that was disclosed in legacy versions of FortiOS," the company said in a new blog post.

Customers are strongly advised to upgrade to the newly released FortiAnalyzer version 5.0.12 or 5.2.5, depending on which branch of the software they're using. The 4.3 branch is not affected.

FortiSwitch users should upgrade to version 3.3.3 and FortiCache users to version 3.0.8 or to the 3.1 branch, which is not affected.

The company has also provided manual workarounds for affected devices that cannot be immediately upgraded. These consist mainly of disabling SSH access to the devices and using the Web-based management interfaces instead.

"As previously stated, this vulnerability is an unintentional consequence of a feature that was designed with the intent of providing seamless access from an authorized FortiManager to registered FortiGate devices," the company said. "It is important to note, this is not a case of a malicious backdoor implemented to grant unauthorized user access."





Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virtual Total
svchost.exe	0.01	5,152 K	11,132 K	1632	Host Process for Windows S...	Microsoft Corporation	0.56
svchost.exe	0.01	4,060 K	9,400 K	1900	Host Process for Windows S...	Microsoft Corporation	0.56
svchost.exe	0.01	3,324 K	1,300 K	1908	Host Process for Windows S...	Microsoft Corporation	0.56
MsMpEng.exe	0.38	115,688 K	59,884 K	1972	Antimalware Service Execut...	Microsoft Corporation	0.58
svchost.exe	0.01	29,836 K	6,064 K	2928	Host Process for Windows S...	Microsoft Corporation	0.56
SearchIndexer.exe	0.03	29,456 K	20,184 K	4020	Microsoft Windows Search I...	Microsoft Corporation	0.58
SearchProtocolHost.exe		1,348 K	6,248 K	2732	Microsoft Windows Search P...	Microsoft Corporation	0.57
SearchFilterHost.exe		1,100 K	5,784 K	4596	Microsoft Windows Search F...	Microsoft Corporation	0.56
SearchProtocolHost.exe		1,840 K	9,660 K	2972	Microsoft Windows Search P...	Microsoft Corporation	0.57
MsDm.exe		8,640 K	7,068 K	436	Microsoft Network Realtime I...	Microsoft Corporation	0.58
svchost.exe		2,012 K	1,468 K	2524	Host Process for Windows S...	Microsoft Corporation	0.56
svchost.exe		1,088 K	2,968 K	4920	Host Process for Windows S...	Microsoft Corporation	0.56
lsass.exe	0.01	4,368 K	6,948 K	532	Local Security Authority Proc...	Microsoft Corporation	0.56
csrss.exe		1,036 K	604 K	428	Client Server Runtime Process	Microsoft Corporation	0.58
winlogon.exe		1,508 K	1,088 K	476	Windows Logon Application	Microsoft Corporation	0.56
LgpnUI.exe		16,540 K	4,112 K	744	Windows Logon User Interfa...	Microsoft Corporation	0.57
dm.exe		12,608 K	2,896 K	752	Desktop Window Manager	Microsoft Corporation	0.56
csrss.exe	0.58	1,356 K	2,360 K	2468	Client Server Runtime Process	Microsoft Corporation	0.58
winlogon.exe		1,724 K	1,736 K	2500	Windows Logon Application	Microsoft Corporation	0.56
dm.exe	1.90	42,628 K	70,268 K	2604	Desktop Window Manager	Microsoft Corporation	0.56
explorer.exe	0.11	53,512 K	89,980 K	3232	Windows Explorer	Microsoft Corporation	0.56
MSASQCu.exe		5,500 K	7,640 K	5396	Windows Defender User Inte...	Microsoft Corporation	0.58
minikatz.exe		1,608 K	6,940 K	3400	minikatz for Windows	gentilkiwi (Benjamin DELPY)	13.54
conhost.exe		10,408 K	13,080 K	5340	Console Window Host	Microsoft Corporation	0.58
process.exe		2,320 K	8,960 K	5408	Systematic Process Explorer	Systematic - www.systematic.co.uk	0.58
process64.exe	3.11	14,208 K	37,932 K	4872	Systematic Process Explorer	Systematic - www.systematic.com	0.58
OneDrive.exe	0.06	4,784 K	3,136 K	5644	Microsoft OneDrive	Microsoft Corporation	0.56
MsMpEng.exe		2,764 K	1,992 K	3388	Microsoft Malware Protection...	Microsoft Corporation	0.56

Best way to check for malware


The company is likely trying to differentiate this problem from an SSH backdoor found recently in network firewalls from Juniper Networks, one of its competitors. In Juniper's case, the backdoor was added to the company's source code without its knowledge and remained undetected for two years. That incident is reportedly being investigated by the FBI.



Lucian Constantin — *Romania Correspondent*



You Might Like

Promoted Links by Taboola 

Fatherhood's Changed Prince William

Reuters TV

使用当地通讯卡让泰国旅行更加轻松



Carophile

[Sign In](#) | [Register](#)

The Ultimate Way to Get Cheap Hotel Rooms

Hotel Bargains

5 traits of successful developers

Intel

Brunch Like a Local in NYC

AFAR

Homido turns just about any smartphone into a VR headset

NSFW: T-Mobile hurls insults at competitors AT&T, Verizon and Sprint

Drone buying guide 2015

So You Want to Sweat? 8 Life Hacks for Staying Fit with MS

Living Like You by Novartis

Copyright © 1994 - 2016 CXO Media, Inc. a subsidiary of IDG Enterprise. All rights reserved.