

#### 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.

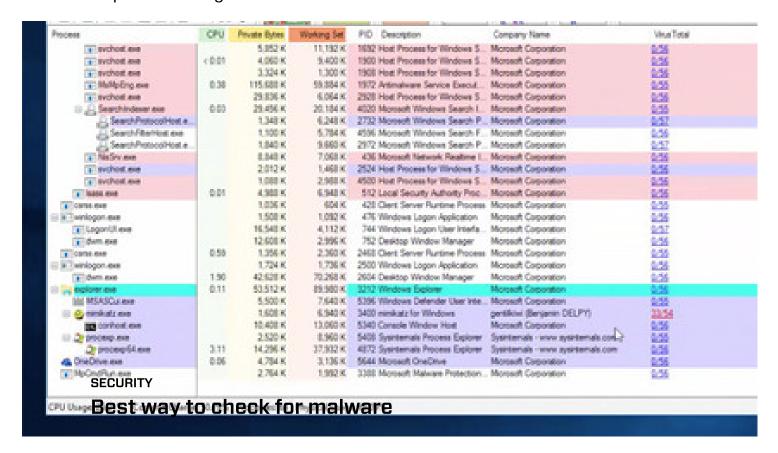
"These versions have the same management authentication issue that was disclosed in legacy versions of FortiOS," the company said in a new blog post.

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 <u>provided manual workarounds</u> 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."



The company is likely trying to differentiate this problem from <u>an SSH backdoor found recently</u> 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.



Insider: 10 Tough Security Interview Questions, and How to Answer Them



## You Might Like

Promoted Links by Taboola D

## **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.