WEA

HARD S IN

FORT

Multiple) and hardcoded cryptographic keys to communicate with the FortiGuard Web Filter, AntiSpam and AntiVirus cloud services. This allows attackers to eavesdrop on user activity and manipulate server responses.

VENDOR DESCRIPTION

"From the start, the Fortinet vision has been to deliver broad, truly integrated, high-performance security across the IT infrastructure.

We provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines Security Processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control–while providing easier administration."

Source: **https://www.fortinet.com/corporate/about-us/about-us.html**

BUSINESS RECOMMENDATION

The vendor provides a patch and users of affected products are urged to immediately upgrade to the latest version available.

VULNERABILITY OVERVIEW/DESCRIPTION

Fortinet products, including FortiGate and Forticlient regularly send information to Fortinet servers (DNS: guard.fortinet.com) on

- UDP ports 53, 8888 and
- TCP port 80 (HTTP POST /fgdsvc)

This cloud communication is used for the FortiGuard **Web Filter** feature, FortiGuard **AntiSpam** feature and FortiGuard **AntiVirus** feature.

The messages are encrypted using XOR "encryption" with a static key. The protocol messages contain the following types of information:

Serial nu + unique ID)
This info nternet traffic to

- le ization us E
- le ation
- us track an in he

Full HTT)

This info nternet traffic to inspecti communication are sent via this protocol, effectively breaking the confidentiality of SSL/TLS.

Unspecified email data (AntiSpam feature)

We do not have any further information on what kind of information is sent by the AntiSpam feature.

Unspecified AntiVirus data (AntiVirus feature)

We do not have any further information on what kind of information is sent by the AntiVirus feature.

By intercepting and manipulating internet traffic an attacker can manipulate the responses for FortiGuard Web Filter, AntiSpam and AntiVirus features.

PROOF OF CONCEPT

The following Python 3 script decrypts a FortiGuard message (the static XOR key has been removed from this advisory).

```python
from itertools import cycle

def forti_xor(s1):
    xor_key = **removed**
    message = ''.join(chr(c ^ k) for c, k in zip(s
1, cycle(xor_key)))
    return message

r1=bytes.fromhex('6968766f606e776c2d2d21262138475c5
b5a475b545e475c6b6a776b646e776c6b6a772b646e776c6b6a
776b646e776c6b6a776bbadf04036b6a776c616a846f')
```

```
print
```

In this ca

```
'\x02
00\x0
\x00\
```

```
000\x
0\x00
```

Another

```
'\x02
\...x
om/\x
```

```
0\x00
oft.c
```

VULN

The following FortiOS versions are affected according to the vendor:

- FortiOS 6.0.7 and below (Update 2019-11-27: According to Fortinet, also v6.0.7 is affected)
- FortiClientWindows 6.0.6 and below
- FortiClientMac 6.2.1 and below

The security advisory of the vendor can be found at:
https://fortiguard.com/psirt/FG-IR-18-100

VENDOR CONTACT TIMELINE

2018-05-17	Contacting vendor through psirt@fortinet.com, sending advisory with public PGP key
2018-05-17	Auto-Response: “Thank you for contacting us regarding your inquiry. We have created a PSIRT ticket for this inquiry”
2018-05-17	Response: “Thank you to report us this vulnerability. I created an internal incident and I will communicate further with you while I’m investigating the impact of this.”
2018-05-28	Requesting update, “If we don’t get an appropriate response (see my initial email) by the end of next week, we will consider disclosing the vulnerability without further coordination.”
2018-05-28	Auto-Response: “Thank you for contacting us regarding your inquiry. We have created a PSIRT ticket for this inquiry”
2018-06-05	Requesting update again, “This is the final attempt to contact you”, plus reaching out to Fortinet via Twitter, LinkedIn.
2018-06-05	First response after 3 weeks, developers are working on a fix, “Please therefore kindly wait for

SOLUTION

The vendor provides updated versions for the affected products:

- FortiOS 6.2.0 (Update 2019-11-27: According to Fortinet, only 6.2.0 includes the patch, not the previously stated v6.0.7)
- FortiClientWindows 6.2.0
- FortiClientMac 6.2.2

The security advisory of the vendor can be found at:
https://fortiguard.com/psirt/FG-IR-18-100

WORKAROUND

None.

ADVISORY URL

https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html

EOF Stefan Viehböck / @2019

TITLE
FortiGuard XOR Encryption

PRODUCT
Multiple Fortinet Products (see Vulnerable / tested versions)

VULNERABLE VERSION
Multiple (see Vulnerable / tested versions)

FIXED VERSION

Multiple

CVE NUM
CVE-201

IMPACT
High

HOMEPA
https://w

FOUND
2018-05-

BY
Stefan V

SEC Consult is one of the leading consultancies in the field of cyber and application security. The company specializes in information security management, security audits, penetration testing, ISO 27001 certification support, cyber defense and secure software certification.