PTA Security Advisory-No: 60

07-November-2019

Threat Classification: Remote Code Execution Vulnerability

Name: Fortinet FortiManager and FortiOS VM Remote Code Execution Vulnerability (CVE-2019-6695, CVE-2019-5587)

Affected Systems: Affects the following products of Fortinet:

- FortiOS VM
- FortiManager VM

Distribution: The vulnerabilities can be exploited in the following versions of Fortinet product:

Product Name	Affected Versions	Resolved Product and Version
Fortinet FortiOS VM	all below 6.0.5	FortiOS VM versions 6.2.0
Fortinet FortiManager VM	all below 6.2.1	FortiManager VM version 6.2.1

Summary:

Due to the lack of root file system integrity check in the above mentioned Fortinet products, an attacker may get read/write access for the VM image (before it is booted up) to implant third-party programs by recreating the image through specific methods.

Attack Severity	Critical
Attack Vector	Network
Attack Type	Remote code execution
Privileges Required	None

Further details are available at following official link: https://fortiguard.com/psirt/FG-IR-19-017

Recommendations:

- For official recommended upgrade path, visit following website link to fix the aforementioned vulnerabilities:

  https://docs.fortinet.com/upgrade-tool

- In all cases, ensure availability of stable version, before upgrade, by the relevant vendor.

- Whenever required, access security system with minimal access rights and privileges.

- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Only use licensed software and avoid download/use of cracked and pirated software.

- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.

- In case of any incident, please report to this office.