Tonga National Computer Emergency Response Team

Windows Denial of Service Vulnerability

Dear Constituents,

Microsoft released a security advisory about a denial-of-service vulnerability that could render multiple versions of Windows completely unresponsive.

The vulnerability affects all versions of Windows 7 through 10 (including 8.1 RT), Server 2008, 2012, 2016, and Core Installations that don't have the latest set of security updates released as part of the September 2018 Patch Tuesday updates.

How it works

IP fragmentation attacks are a known form of **denial of service**, where the victim computer receives multiple IP packets of a smaller size that are expected to be reassembled into their original form at the destination.

FragmentSmack is a TCP fragmentation type of attack, also known as a Teardrop attack, that prevents reassembling the packets on the recipient end. The vulnerability is as old as Windows 3.1 and 95, where it crashed the OS, but it was seen in the more recent Windows 7, too.

"An attacker could send many 8-byte sized IP fragments with random starting offsets, but withhold the last fragment and exploit the worst-case complexity of linked lists in reassembling IP fragments," reads Microsoft's advisory on the bug.

The effect is that the CPU of the machine reaches maximum utilization level and renders the operating system unresponsive. As soon as the packet salvo ceases, the CPU returns to normal usage and the system recovers.

Microsoft recommends disabling packet reassembly

If the environment does not allow applying the security updates immediately, Microsoft recommends using the commands below to disable packet reassembly as a workaround for the FragmentSmack denial-of-service bug:

```
Netsh int ipv4 set global reassemblylimit=0
Netsh int ipv6 set global reassemblylimit=0
```

They will drop any packets that are out of order, increasing the potential of losses. To avoid any problems there should not be more than 50 out-of-order packets.

Some security products from CheckPoint are also affected by FragmentSmack.

Affected Products of Windows, you can click on the link below:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180022

What to do

1. Apply security updates as required by the Microsoft Products
2. The following commands disable packet reassembly. Any out-of-order packets are dropped. There is a potential for packet loss when discarding out-of-order packets. Valid scenarios should not exceed more than 50 out-of-order fragments.

   Microsoft recommend testing prior to updating production systems.

```
Netsh int ipv4 set global reassemblylimit=0
Netsh int ipv6 set global reassemblylimit=0
```

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: report@cert.to
web: www.cert.to