Install the patch immediately for Windows Server & Windows 10 to run IIS so that it will not be attacked by DOS

Windows Server and Windows 10 servers running Internet Information Services (IIS) easily become targets of denial of service (DOS) attacks.

Recently, Microsoft has posted a warning message regarding security issues on its security response center (Security Response Center), with content related to Windows Server and Windows 10 servers being Running Internet Information Services (IIS) easily becomes the target of denial of service (DOS) attacks.

More precisely, all IIS servers running Windows Server 2016, Windows Server Version 1709, Windows Server Version 1803, as well as Windows 10 (versions 1607, 1703, 1709 and 1803) are affected by This DoS incident.

The vulnerability described in Microsoft's ADV190005 security recommendation allows a potential remote attacker to activate the DoS status by taking advantage of the IIS resource exhaustion error, which means it "can temporarily cause System CPU usage spikes 100%, at least until malicious connections are actually removed entirely by IIS '.

These malicious agents can launch DoS attacks against vulnerable Windows servers by sending multiple HTTP / 2 requests manually.

1. Use an 8-character Windows NTLM password? Congratulations, your password may be unlocked after only 2.5 hours

Microsoft also advises that there is no mitigation or solution for the vulnerability reported by Gal Goldshtein of F5 Networks, and they recommend that all users install February updates that are not covered. The secret listed

in the table below is as follows:

Version Version Patch Windows 10 Version 1607 for 32-bit Systems 4487006 Windows 10 Version 1607 for x64-based Systems 4487006 Windows 10 Version 1703 for 32-bit Systems 4487011 Windows 10 Version 1703 for x64-based Systems 4487011 Windows 10 Version 1709 for 32-bit Systems 4487021 Windows 10 Version 1709 for 64-based Systems 4487021 Windows 10 Version 1709 for ARM64-based Systems 4487021 Windows 10 Version 1803 for 32-bit Systems 4487029 Windows 10 Version 1803 for ARM64-based Systems 4487029 Windows 10 Version 1803 for x64-based Systems 4487029 Windows Server 2016 4487006 Windows Server 2016 (Server Core installation) 4487006 Windows Server, version 1709 (Server Core installation) 4487021 Windows Server, version 1803 (Server Core installation) 4487029

Details are given in Microsoft's ADV190005 security recommendation as follows:

"HTTP / 2 allows the client to specify any number of SETTINGS frames with any number of SETTINGS parameters. However, in some cases, excessive installation may cause services to become unstable. and thus lead to CPU usage temporarily spike until the connection time runs out and the connection is closed ".

As a way to improve the situation, Redmond's security team "has added the ability to specify thresholds for the number of HTTP SETTINGS / 2 in the request", threshold levels must be set by the IIS administrator after evaluation. The environment and HTTP / 2 on their systems require protocols, as they will not be preconfigured by Microsoft.

1. MySQL vulnerabilities allow malicious servers to steal data from customers

To set these limits, Microsoft has added the following registry entries to vulnerable Windows 10 releases:

Path:

```
ComputerHKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesHTTPParameters
```

Name : Http2MaxSinstallPerFrame

Type : DWORD

Data : The minimum supported value is 7 and up to 2796202. Value outside the range is cut to the corresponding minimum / maximum end value.

Path:

```
ComputerHKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesHTTPParameters
```

Name : Http2MaxSettingsPerMinute

Type : DWORD

Data : The minimum supported value is 7. The smaller value is cut to the minimum value.

After the thresholds are placed on the Windows system running IIS, the connections will be immediately canceled if:

1. If a single Setting frame contains more settings than the "Http2MaxSinstallPerFrame" value.
2. If the number of parameter settings in many Setting frames is received within one minute, pass the "Http2MaxSinstallPerMinute" value.

Besides, according to Microsoft, it should be noted that you may have to restart the service or restart the server so that the newly added registry values ??can be read.

1. Microsoft shook hands with VirusTotal in resolving malicious code issues that affected MSI files

Running Windows servers that were previously exploited by the attacker with the help of zero-day in IIS 6.0 will affect WebDAV services by default in all IIS distributions, from July 7 2016 to March 2017.