Microsoft fixes a serious vulnerability that has existed for 17 years in Windows Server

The vulnerability has tracking code CVE-2020-1350 and its official name is SIGRed. It has been in Windows DNS Server for nearly two decades and has only recently been successfully handled by the efforts of Microsoft experts with help from the Checkpoint Security security team.

The reason why SIGRed is rated at maximum severity, 10 out of 10, is because it is a remote code execution vulnerability that directly affects a wide range of Windows Server editions (from 2003 to 2019).), and in the case of successful exploitation, SIGRed will pave the way for hackers to take over Domain Administrator privileges, thereby acquiring the entire infrastructure of the victim's organization / business.

In addition, SIGRed is also dangerous at the 'malware characteristics' it possesses, meaning that a successful exploit session could automatically propagate to other vulnerable Windows systems across the network. No need for user interaction as a bridge. This feature puts it on a par with the serious well-known vulnerabilities that have been recorded as EternalBlue in Server Message Block (SMB) and BlueKeep on Remote Desktop Protocol (RDP).

SIGRed

SIGRed vulnerability

The Domain Name System (DNS) can be thought of as the 'telephone directory' of the Internet, allowing clients to connect to the server to access resources. This model maps domain names to IP addresses to allow connecting to the right query server.

Researchers at Check Point Security have discovered a flaw in Microsoft's DNS implementation that could be exploited when the server parses an incoming query or responds to a forwarded request. They found an integer overflow that led to a heap-based buffer overflow in 'dns.exe! SigWireRead' - a function that analyzes feedback types for SIG queries.

So basically, it is possible to exploit the vulnerability in the target DNS server by answering one of its queries with a SIG response large enough to trigger the error. In addition, the researchers found that a SIGRed exploit does not need to be on the same network as the destination DNS server, because DNS data can be transmitted over TCP connections, supported by Windows DNS. . As such, the destination server analyzes the data as a DNS query even if it is sent as an HTTP payload.

Besides, because the Windows DNS server supports 'Connection Reuse' and 'Pipelining', an attacker can launch some queries over TCP connection without waiting for a reply.

The flaw has existed for 17 years

This vulnerability has existed in Microsoft's code for over 17 years, and the patch was only released by Microsoft on July 14. In the event that the patch cannot be applied at this time, Microsoft recommends that the system administrator modify the registry to minimize the problem. The change takes effect after restarting the DNS service:

```
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesDNSParameters DWORD = TcpReceiv
```

After applying the patch, the administrator should revert to the original state changes by deleting the TcpReceivePacketSize value and its data.

Download the patch here