THREAT BRIEF

Gartner

COOL VENDOR 2020™

SigRed (CVE-2020-1350)

Preventing a Wormable Domain Name System Vulnerability in Microsoft Servers • Summer 2020

SigRed is a vulnerability in Microsoft's Domain Name System (DNS) Server software that was discovered by security researchers at Check Point. The vulnerability, which has been assigned CVE-2020-1350, is present in the parsing of specific DNS resource records of the Signature (SIG) type, leading to a buffer overflow and Remote Code Execution (RCE). This vulnerability affects Windows DNS servers specifically, and the vulnerable code is present in Windows OS versions up to 17 years back. Initial proofs-of-concept for scanning vulnerable DNS servers over the internet have been developed by security researchers, and adversaries are undoubtedly working to develop actual working exploits.

SigRed is considered "wormable" because it requires no user interaction to trigger, much like BlueKeep, ETERNALBLUE, and SMBGhost exploits that have previously made headlines (all of which Trinity Cyber defeats). These vulnerabilities present a unique challenge to defenders because they are easily incorporated into malware that automatically spread to infect other machines. This can happen via internet-to-internet and even within the boundaries of a corporate network. As an unauthenticated RCE, SigRed presents a massive dilemma—patch quickly, or figure out how to detect and act on vulnerable DNS responses at a network level.

Halting the Spread of Malware

Trinity Cyber detects SigRed exploits within a fully parsed DNS session by comparing the calculated size of several important fields within a SIG resource record query response, which are overflowed during exploitation. Our detection methodology doesn't rely on static indicators like IP addresses or domains and doesn't rely on black or whitelisting to be effective.

When SigRed exploitation is detected, our advanced threat prevention service acts immediately by closing the network session. This prevents malicious SigRed responses from exploiting a vulnerable or unpatched Windows DNS server.

Trinity Cyber's immediate actions in flight protect our clients from SigRed vulnerabilities, even if they haven't had time to patch their DNS servers yet.

sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

Trinity Cyber