Alert – Microsoft Windows DNS Servers Vulnerabilities

Description:

Microsoft Windows Domain Name System (DNS) servers are vulnerable to heap overflow attacks. *Microsoft acknowledges* that *"an attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account."* This remote code execution vulnerability exists in Windows DNS servers when they fail to properly handle requests.

Impact of the vulnerabilities:

Windows servers that are configured as DNS servers are at risk from this vulnerability. A successful attack could allow the execution of arbitrary code. *Symantec also* notes that an unsuccessful attack results in a denial-of-service. Successful exploitation could enable unauthenticated attackers to send malicious requests to affected servers. And by using compromised credentials, an attacker can modify the location to which an organization's domain name resources resolves. This enables the attacker to redirect user traffic to attacker-controlled infrastructure and obtain valid encryption certificates for an organization's domain names, enabling man-in-the-middle attacks.

Vulnerable or affected versions:

All Microsoft Windows Domain Name System (DNS) servers

Solution:

Rw-CSIRT is strongly recommending **users** to:

Update their software installations to the latest versions by following the instructions below.
The latest product versions are available to end users via one of the following methods:

- Users can update their product installations manually by choosing Help > Check for Updates.
- The products will update automatically, without requiring user intervention, when updates are detected.

For **IT administrators** (managed environments):

Please review FireEye's blog on global DNS infrastructure hijacking for more information. Additionally, Rw-CSIRT recommends the following best practices to help safeguard networks against this threat:

- Implement multifactor authentication on domain registrar accounts, on administration portal or on other systems used to modify DNS records.
- Verify that DNS infrastructure (second-level domains, sub-domains, and related resource records) points to the correct Internet Protocol addresses or hostnames.
- Search for encryption certificates (SSL) related to domains and revoke any malicious certificates.
- Validate A and NS record changes. Also validate the source IPs in OWA/Exchange logs.
- Conduct an internal investigation to assess if attackers gained access to your environment.

Affected users should: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

Vulnerability Details:
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

References:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8626
- https://cwe.mitre.org/data/definitions/122.html
- https://www.symantec.com/security-center/vulnerabilities/writeup/106076
- https://www.us-cert.gov/ncas/current-activity/2018/12/11/Microsoft-Releases-December-2018-Security-Updates

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.