Security Advisory 2021-005

Use of Remote Desktop Protocol in DDoS Attacks

January 26, 2021 — v1.0

TLP:WHITE

History:

- *26/01/2021 — v1.0 – Initial publication*

Summary

DDoS attacks were observed recently, where Microsoft Remote Desktop Protocol (RDP) was abused in order to reflect and amplify the amount of bandwidth involved. This is not a vulnerability by itself, but an abuse of the RDP protocol design [1]. Attacks using this technique were observed with sizes range from 20-750 Gbps [2].

Technical Details

The Remote Desktop Protocol (RDP) service is included in Microsoft Windows operating systems. It provides authenticated remote access to Windows-based workstations and servers. RDP can be configured to run on TCP and/or UDP. By default both use port 3389.

When enabled on UDP, the Microsoft Windows RDP service may be abused to launch UDP reflection/amplification attacks with an amplification ratio of 85.9:1. The amplified attack traffic consists of non-fragmented UDP packets sourced from UDP/3389 and directed towards the destination IP address(es) and UDP port(s) of the attacker's choice.

The collateral impact of RDP reflection/amplification attacks affects also the organizations whose Windows RDP servers are abused as reflectors/amplifiers. This may include partial or full interruption of mission-critical remote-access services, as well as additional service disruption due to transit capacity consumption, state-table exhaustion of stateful firewalls, load balancers, etc. Filtering of all UDP/3389-sourced traffic by network operators may potentially block also legitimate traffic, including legitimate RDP remote session replies [2].

Affected Products

Microsoft RDP server instances exposed on the Internet.

Recommendations

It is recommended that RDP servers to be accessible only via VPN services in order to protect them against this attack, but also against other types of abuse[5]. Alternatively RDP traffic can be tunneled through SSH as described in [3].

Allowing RDP only on TCP, filtering IP sources, and changing the listening port for RDP can be considered as mitigation measures [4, 5].

References

[1] https://arstechnica.com/information-technology/2021/01/ddosers-are-abusing-microsoft-rdp-to-make-attacks-more-powerful/

[2] https://www.netscout.com/blog/asert/microsoft-remote-desktop-protocol-rdp-reflectionamplification

[3] https://www.saotn.org/tunnel-rdp-through-ssh/

[4] https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/change-listening-port

[5] https://www.techrepublic.com/article/how-to-better-secure-your-microsoft-remote-desktop-protocol-connections/