UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00095

MICROSOFT RDP USED IN DDOS ATTACKS

DATE ISSUED: 26th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Netscout researchers has discovered the possibility of existing servers to flood networks with traffic in DDoS style attacks by abusing Microsoft's Remote Desktop Protocol (RDP) using UDP reflection and amplification.

BREAKDOWN

14,000 servers with service enabled on port 339 for both standard UDP and TCP have been identified as potential vessels to perform DDoS attacks using a ration of 85.9:1 in UDP reflection/amplification attacks. It has been discovered that "booters" or groups that perform DDoS for hire services have opened up this potential attack vector to the 'general attack population'. By targeting an IP address, attackers can send enormous UDP packets, padded by appending numerous zero's, to flood and disable a network by abusing RDP's remote authentication and Virtual Desktop Infrastructure (VDI). DDoS attacks have the potential to cripple or crash systems, removing usability and access to mission critical systems and infrastructure and other general disruption due to transit capacity consumptions.

REMEDIATION STEPS

- Deploy Windows RDP servers behind a VPN concentrator
- Assess all servers to identify any servers that may be susceptible to this form of abuse
- Disable RDP on port 3389 until protection methods can be implemented
- Separate internal and external web server traffic over separate upstream internet transfer links
- Check with you ISP or service provider regarding existing DoS protection measures
- Check server configuration and only permit traffic via required IP protocols and ports

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/threat-actors-can-exploit-windows-rdp-servers-to-amplify-ddos-attacks/163248/
ZDNet	https://www.zdnet.com/article/windows-rdp-servers-are-being-abused-to-amplify-ddos-attacks/
Health Security	https://healthitsecurity.com/news/threat-actors-can-leverage-rdp-servers-to-amplify-ddos-attacks
Syxsense	https://www.syxsense.com/windows-rdp-servers-targeted-in-ddos-attacks