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

CYBER GUIDANCE ISSUE 00099

NEW NAT SLIPSTREAMING ATTACK 2.0

DATE ISSUED: 2nd February 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Chrome, Firefox and Edge vendors have blocked access to eight additional ports following the discovery of the evolution of a NAT Slipstreaming attack, meaning ports 69, 137, 161, 179, 1720, 1723, 6566 and 10080 will have all traffic access blocked in the Chrome browser.

BREAKDOWN

Once a victim has been redirected to a malicious website, a JavaScript code would be used to establish a direct connection to the user's devices which bypasses, or slipstreams, past defences such as firewalls or Network Address Translator (NAT) Tables. Further abuse of this connection could result in further exploitation of the device or an attempt to reach other devices. The first instance of this type of attack abused the Session Initiation Protocol (SIP) using ports 5060 and 5061 which resulted in these two ports being blocked, now a further eight have been added to the list. Rather than take advantage of SIP, this new attack "piggybacks" on the H.323 protocol which are used for multimedia and bypass firewalls and NAT tables. Google has expressed concerns that there will be attempts to abuse other ports and similar protocols in a comparable fashion.

REMEDIATION STEPS

- Upgrade browsers to the latest version to have the new blocks applied.
- Be wary of phishing and other social engineering scams that may lead to malicious websites.
- Educate users on how to spot malicious activity.
- To triage an affected device, take it offline and remove all network connectivity.

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/google-deploys-new-chrome-mitigations-against-new-nat-slipstreaming-attack/
Security Week https://www.securityweek.com/nat-slipstreaming-20-exposes-devices-internal-networks-remote-attacks
Threatpost https://threatpost.com/remote-attackers-internal-network-devices-nat-slipstreaming/163400/