UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00037

## MFA BUGS IN MICROSOFT 365

DATE ISSUED: 21st September 2020

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | [✓ HIGH] |
| EASE OF EXPLOIT | LOW | [✓ MEDIUM] | HIGH |

## OVERVIEW

Researchers at Proofpoint have uncovered a bug in Microsoft's 365, formerly Office 365, multi-factor authentication system enabling attackers to bypass the WS-Trust security and access cloud applications.

## BREAKDOWN

Enabled in Microsoft 365 Cloud environments, WS-Trust is an OASIS standard for extensions that validate and replenish security tokens with the objective of establishing trust relationships, and is considered inherently insecure. The design of the session login may allow an attacker to gain full access to a user's account. One of such circumstances is the spoofing of an IP address and using header manipulation, bypass the MFA. All connections are recognised as "Modern Authentication" due to capabilities for compatibility with legacy systems. With MFA becoming necessity to security, especially with the swift uptake in remote working due to Covid-19 making it an increasingly appealing target for attackers.

## REMEDIATION STEPS

- Ensure legacy systems are updated to use Modern Authentication
- Combine MFA with threat visibility and cloud monitoring technologies to alert on unusual activities
- Install the latest security patches provided by Microsoft across all systems as soon as they are available.
- Be wary when granting access permission to applications in your cloud environment.

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost: | https://threatpost.com/flaws-in-microsoft-365s-mfa-access-cloud-apps/159240/ |
| Tech Radar: | https://www.techradar.com/nz/news/new-vulnerabilities-allow-hackers-to-bypass-mfa-for-microsoft-365 |