U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00203

MS EXCHANGE CREDENTIAL LEAK IN AUTODISCOVER

DATE ISSUED: 27th September 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Microsoft Exchange Autodiscover protocol – used to assist in the configuration of applications like Microsoft Outlook - has a bug which is causing domain credentials to be leaked in plaintext to external domains in the same TLD (top-level domains).

BREAKDOWN

The leaked email and password credentials could be easily obtained by an attacker who is the owner of one such domain or has the ability to sniff traffic in the same network. Alternatively, a sophisticated DNS Poisoning campaign on a large scale could also draw out credentials over time. This is possible because the flaw in the protocol leaks web requests to other domains if they are in the same TLD e.g. Autodiscover.com which can then be used as a "credential trap" for the leaked, plaintext domain credentials. Over 4 months, investigators from Guardian Core were able to round up 372,072 leaked Windows domain credentials and to further their experiment devised a potential attack that downgrades authentication replacing OAuth or HYLM with HTTP basic authentication which is also sends credentials in clear-text, widening the potential scope of damage. The protocol flaw is old and known to Microsoft and as yet has not been patched, however Microsoft now appear to be purchasing all domain TLDs for Autodiscover in an attempt to mitigate the issue.

REMEDIATION STEPS

- Actively block all Autodiscover domains - a comprehensive list can be found here https://data.iana.org/TLD/tlds-alpha-by-domain.txt or a script prepared by Guardian Core can be run.
- Disable support for basic authentication when deploying or configuring Microsoft Exchange3
- If Autodiscover must remain enabled, ensure it is not able to "fail upwards" or uses the "back off" procedure.
- Change your domain password and use best practices for new passwords

REFERENCES & RESOURCES

Guardian Core	https://www.guardicore.com/labs/autodiscovering-the-great-leak/
Threatpost	https://threatpost.com/exchange-outlook-autodiscover-bug-spills-100k-email-passwords/175004/
CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/microsoft-exchange-autodiscover-exposing-credentials/