ZICTA

For Immediate Release
Thursday, March 18, 2021

Warning to On-Premise Microsoft Exchange Server Users

Zambia Information and Communications Technology Authority (ZICTA) wishes to warn the business community in Zambia that rely on on-premise Microsoft Exchange Server to urgently update their software to protect their systems from cyber-attack.

This follows a recent announcement by Microsoft and Volexity regarding the detection of multiple new exploits used to target vulnerabilities **(CVE 2021- 26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)** in on-premises versions of Microsoft Exchange Servers.

Microsoft Exchange is Microsoft's email server solution which is a piece of software that runs on a server and manages all emails.

In light of the above public announcement, the Authority assesses that hackers are attempting to exploit these vulnerabilities before victims implement the Microsoft updates. The business community is therefore being cautioned that, continual use of unpatched exchange servers or delayed implementation of Microsoft-released updates poses a serious risk to affected systems and has the potential to affect all businesses in Zambia that are currently running the Microsoft Exchange on-premise.

It must be noted that successful exploitation of these vulnerabilities allows an attacker to access victims' Exchange Servers, enabling them to gain persistent system access and control of an enterprise network. The adversaries could continue to exploit this vulnerability to compromise networks and steal information, encrypt data for ransom, or even execute a destructive attack. They may also sell access to compromised networks on the dark web.

The Authority is urging organizations that have identified indications of compromise and do not have the expertise to conduct Digital forensics IOCs or anomalous behaviour to contact its free service for assistance.

Affected Exchange Server versions

The security updates are available for the following operating systems;

- Exchange Server 2010 (update requires SP 3 or any SP 3 RU – this is a Defense in Depth update)
- Exchange Server 2013 (update requires CU 23)
- Exchange Server 2016 (update requires CU 19 or CU 18)
- Exchange Server 2019 (update requires CU 8 or CU 7)

Incident mitigation

Microsoft Exchange Server indicators of compromise (IOCs) include:

a) Presence of web shell code on a compromised Microsoft Exchange on-premises server.
b) Unauthorized access to or use of accounts.
c) Evidence of lateral movement by malicious actors with access to compromised systems.
d) Other indicators of unauthorized access or compromise.

Technical details on how to identify indicators of compromise are available on the Zambia Computer incident Response Team (ZmCIRT) website: ***www.cirt.zm***.

ZICTA has Cyber Security experts specialised in detecting cyber intrusions, digital forensics, risk assessments and incident response.

Issued By:

Ngabo Nankonde (Ms.)
Manager Corporate Communications

Press Contact:
Phone: +260 21 1 378200
For general inquires Email: corporatecommunications@zicta.zm
For Consumer Complaints Email: complaints@zicta.zm
Website: www.zicta.zm
Facebook: ZICTA
Twitter: @ZICTAZM