CTPAT Alert

March 2021

CTPAT ALERT

Cyber Threats – Microsoft Exchange Vulnerabilities

Last Updated: March 17, 2021

To enhance communication with its Members, the Customs Trade Partnership Against Terrorism (CTPAT) program routinely highlights security matters for the purpose of raising awareness and renewing Partners' vigilance in supply chain security. This CTPAT Alert highlights threats posed to Members that utilize on-premises Microsoft Exchange Server.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigations (FBI) released a joint alert relevant to the cyber threat associated with active exploitation of vulnerabilities in Microsoft Exchange on-premises products. The joint alert indicates that several advanced persistent threat (APT) groups are attempting to exploit this vulnerability and target Federal Civilian Executive Branch agencies as well as private companies and academic institutions. CTPAT Members are highly encouraged to take this threat seriously and verify if this alert is applicable to their enterprise. If the alert is relevant to a Member's enterprise, IT staff should begin to follow all applicable steps to mitigate the threats associated with the vulnerabilities laid out in the alert and its corresponding documents.

CTPAT Points of Contact (POC) should ensure that their companies' respective IT Departments are aware of this this serious threat and that corrective actions are taken and documented. Members are encouraged to document any actions taken to remediate this vulnerability and any assistance that may be provided to assist supply chain partners, such as foreign suppliers, freight forwarders, brokers, etc. This information should be made available to the SCSS during the Member's CTPAT Validation to demonstrate compliance with MSC 4.2 and 4.4.

Over the past several months new vulnerabilities have been identified and reported that may affect CTPAT Members and their business partners. It is important for Members to remain vigilant against the persistent threat associated with cyber threat actors. CTPAT Members should continue to ensure personnel are adequately trained, as this is often seen as the first step in mitigating risk associated with employees, contractors and business partners. User authentication procedures should be assessed against the current government and private industry recommendations and all critical security updates (patches) should be deployed as quickly as possible. POC's should ensure that IT personnel identify vulnerabilities and deploy patches in a timely manner. Several of the most recent and significant breaches that have been reported were attributable to a lack of adequate user authentication procedures and failure to deploy critical patches to affected solutions in companies' networks.

Relevant Links: Compromise of Microsoft Exchange Server FBI/CISA Joint Advisory

U.S. CERT/CISA – Remediating Microsoft Exchange Vulnerabilities

CTPAT Cyber MSC Videos (YouTube)

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229