Illinois Department of Insurance

JB PRITZKER
Governor

DANA POPISH SEVERINGHAUS
Acting Director

TO: All Regulated Entities

FROM: Dana Popish Severinghaus, Acting Director

DATE: May 5, 2021

RE: **Company Bulletin 2021-07**
Microsoft Exchange Vulnerability Notification

The purpose of this bulletin is to alert regulated entities to Microsoft Exchange vulnerabilities that the Department has been made aware of. Regulated entities should immediately assess their exposure and take steps to remediate any weaknesses.

On March 2, 2021, Microsoft released emergency out-of-band security updates to address four zero-day vulnerabilities affecting Microsoft Exchange Servers. The vulnerabilities, tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, impact Microsoft Exchange Servers which are used to enable on-premise use of MS products (MS Outlook). Successful exploitation of these vulnerabilities allows an attacker to access on-premise Exchange Servers, enabling them to gain persistent system access and control of an enterprise network. These vulnerabilities are not known to impact Exchange online or Microsoft 365 cloud email services.

On April 13, 2021, Microsoft released a software update to mitigate significant vulnerabilities that affect on-premise Exchange Servers 2013, 2016, and 2019. An attacker could use these vulnerabilities to gain access and maintain persistence on the target host. These vulnerabilities are different from the ones disclosed and fixed in March 2021 – the security updates released in March 2021 will not remediate against these vulnerabilities. Given the powerful privileges that Exchange manages by default and the amount of potentially sensitive information that is stored in Exchange Servers operated and hosted by (or on behalf of) federal agencies, Exchange Servers are a primary target for adversary activity.

Regulated entities should immediately assess the risk to their systems and consumers and take steps necessary to address vulnerabilities and customer impact. The assessment should identify internal use of vulnerable Microsoft Exchange products and any use of these products by critical third parties.

Regulated entities should immediately patch or disconnect vulnerable servers, and use the tools provided by Microsoft to identify and remediate any compromise exploiting these vulnerabilities. Regulated entities should also continue to track developments in this compromise and respond quickly to new information.

The U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency ("CISA") has released a current activity update outlining how to search for a compromise and, in response to the newly disclosed vulnerabilities, issued Supplemental Direction Version 2 to Emergency Directive (ED) 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities. ED 21-02 Supplemental Direction V2 requires federal departments and agencies to apply Microsoft's April 2021 Security Update to mitigate against these significant vulnerabilities affecting on-premises Exchange Server 2016 and 2019.