Prevalent™

Third-Party Microsoft Exchange Server ProxyLogon Vulnerability Assessment

Prevalent

Contents

Prevalent

Document Purpose

This document provides example questions that can be leveraged to assess the risk among third parties (e.g., vendors, partners, suppliers, etc.) related to Microsoft Exchange Server ProxyLogon vulnerability announced in March 2021. The goal of the survey is to provide you with visibility into whether the organization has been impacted by the ProxyLogon vulnerability and the level of impact it had on client information or data held by the organization. The survey aims to provide assurance to clients that the recommended steps have been taken to mitigate and respond to the attack, through implementing appropriate controls as identified through the security guidelines from Microsoft. Questions are provided as either multiple choice, free text, or single selection.

Sample Questions for Third Parties

	Question	Potential Responses
1	Has the organization been impacted by the recent Microsoft Exchange ProxyLogon vulnerability? *(Please select one)*	☐ Yes, we have been impacted as a result of the recent Microsoft Exchange ProxyLogon vulnerability. ☐ No, we have not been impacted as a result of the recent Microsoft Exchange ProxyLogon vulnerability. ☐ The organization is unsure if it has been impacted as a result of the recent Microsoft Exchange ProxyLogon vulnerability.
2	Has the organization implemented patches recently released by Microsoft to the affected systems? *(Please select one)*	☐ Yes, the organization has obtained, tested and successfully installed the patches released by Microsoft. ☐ No, the organization has not yet obtained, tested and installed the patches released by Microsoft. ☐ The organization is unable to install the updates provided by Microsoft.
3	If the organization is unable to install the recommended updates, have the following actions been taken based off of Microsoft's proposed Server Vulnerabilities Mitigations? *(Please select all that apply)*	☐ Implement an IIS Re-Write Rule to filter malicious https requests. ☐ Disable Unified Messaging (UM). ☐ Disable Exchange Control Panel (ECP) VDir. ☐ Disable Offline Address Book (OAB) VDir. ☐ The organization is unable to apply any of the mitigations recommended by Microsoft.

	Question	Potential Responses
4	If the organization is unable to install the recommended updates or apply the mitigations recommended by Microsoft, have the following actions been taken? (*Please select all that apply)*	☐ Blocking untrusted connections to the Exchange server port 443. ☐ Where secure remote access solutions are already in place configuring Exchange only to be available remotely via this solution.
5	Has the organization proactively searched systems for evidence of compromise, in line with Microsoft guidance? (*Please select all that apply)*	☐ The organization is using the 'Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities' to aid in remediation activities. ☐ The organization has installed the Microsoft Exchange On-premises Mitigation Tool (EOMT) as a means of identifying systems for evidence of compromise. ☐ The organization has consulted the TLP WHITE advisory paper from CISA and the FBI a means of further investigating and mitigating the vulnerabilities.
6	Does the organization have an incident investigation and response plan in place? (*Please select all that apply)*	☐ The organization has a documented incident management policy. ☐ The incident management policy includes rules for reporting information security events and weaknesses. ☐ An incident response plan is developed as part of incident investigation and recovery. ☐ Incident response planning includes escalation procedures to internal parties, and communication procedures to clients.
7	Who is designated as the point of contact who can answer additional queries? *(Free text)*	

	Question	Potential Responses
8	What is the level of impact to client systems and data following this vulnerability? *(Please select one)*	☐ There has been no impact to client systems or data following this vulnerability. ☐ There has been a low impact to client systems or data following this vulnerability. ☐ There is a high level of impact to client systems or data following this vulnerability. ☐ There has been significant impact to client systems or data following this vulnerability.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the entire vendor lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.