SONTIQ

IdentityForce. CYBERSCOUT EZShield

URGENT

CLIENT ALERT: MICROSOFT EXCHANGE VULNERABILITY

THIS IS A SECURITY INCIDENT THAT PRIMARILY HITS BUSINESSES.

HERE'S WHAT HAPPENED

In attacks that may have started as early as January 3rd, 2021, more than 30,000 Microsoft Exchange email servers have already been hit and continue to be targeted by hackers due to the volume of email information they hold about an organization. Microsoft recently announced the release of several security updates for the Microsoft Exchange Server, addressing a **"zero-day" vulnerability**.

Microsoft's advice extends to an immediate update of all affected servers, which include:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

According to a ZDNet article, the bugs are being tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Microsoft, **which issued emergency patches, indicated they are "limited targeted attacks" but warned they could be more widely exploited in the near future.**

History suggests many organizations do not update their software when vulnerabilities are found. In 2020, Microsoft warned Exchange server customers to patch the critical flaw CVE-2020-0688 but found that months afterward, **tens of thousands of Exchange servers remained unpatched.**

WHO IS IMPACTED

Microsoft Exchange Server is an email inbox, calendar, and collaboration solution. Users range from the largest enterprises to small and medium-sized businesses worldwide.

FOR BUSINESSES

Apply Fixes Immediately | Microsoft has urged IT administrators and customers to apply the security fixes immediately. For your convenience, we have included this information above, but please access Microsoft's direct guidance using the aforementioned link. Please note, just because fixes are applied now, this does not mean that servers have not already been compromised. Interim mitigation option guides are also available if patching immediately is not possible.

Script for IT Admins | Microsoft has also published a script on GitHub available to IT administrators to run that includes indicators of compromise (IOCs) linked to the four vulnerabilities. IoCs are listed separately here.

More Updates | On March 8th, 2021, Microsoft released an additional set of security updates that can be applied to older, unsupported Cumulative Updates (CUs) as a temporary measure.

READ THE FBI'S STATEMENT ON THE MICROSOFT SERVER HACK.

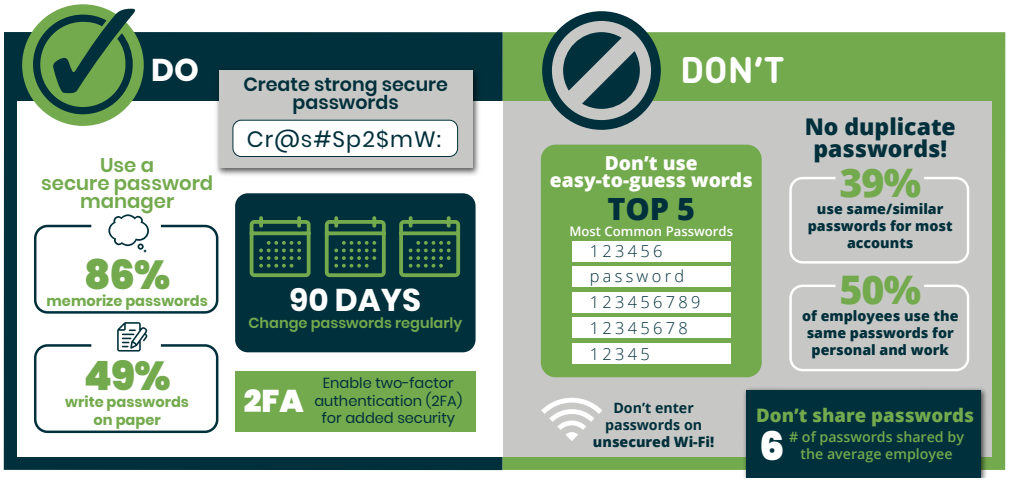
WHAT'S NEXT

On March 2nd, 2021, Microsoft released patches to address the four severe vulnerabilities in Microsoft Exchange Server software. While fixes have been issued, the scope of potential Exchange Server compromise depends on the speed and uptake of patches — and the number of estimated victims continues to grow.

RECOMMENDATIONS & NEXT STEPS

Keep in mind this is a security incident primarily impacting the organization itself. Microsoft has released limited guidance on remediation. Affected organizations should ensure that on-premise Exchange services are ONLY accessible through successful authentication through VPN. There are other proactive measures individuals can take immediately. Changing passwords on your computer, today, is an important step, while also being vigilant and watching credit card statements for any indication of fraud or identity theft.

HOW TO SAFEGUARD YOUR PASSWORDS



ABOUT SONTIQ

Sontiq is an Intelligent Identity Security company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq's brands, IdentityForce, Cyberscout, and EZShield provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at www.sontiq.com or engage with us on Twitter, Facebook, LinkedIn, or YouTube.

© 2021 Sontiq, Inc. All other trademarks or trade names are properties of their respective owners. All rights reserved.