

[View this email in your browser](#)

INNOVATING THE DELIVERY OF INFORMATION TECHNOLOGY

IT Solutions for enterprise and SMB verticals



Urgent Notification

Microsoft Exchange Zero-Day Exploits Detected

Microsoft has identified multiple zero-day exploits affecting its Windows Exchange Server Software. The vulnerabilities allow threat actors to access email accounts, usernames and passwords, and to install malware enabling long-term access to the victim's environments. Microsoft's Threat Intelligence center has attributed the attacks to **HAFNIUM**, a group believed to be state-sponsored and operating from China.

Patches to address the problem have been released. Given the severity of this threat, we are recommending immediate remediation.

Regrettably, the remediation requires downtime, and in our experience the estimated time for your server would be <VARIABLE BASED ON ENVIRONMENT> minutes.

We recognize that this is a busy time for most of our clients. For those who cannot risk the possibility of sustaining downtime during business hours, we are making arrangements to schedule application of the fixes outside of normal business hours. Unfortunately, further complicating this matter is the fact that on rare occasions servers may become suspended during the process, requiring an engineer to be granted physical access to complete the process.

We are asking all clients to respond via email with your desired timeslot; Business Hours or After Hours.

-For those who require that the updates be applied outside of normal business hours, we ask that you provide us with the name and number of someone we may contact in the unlikely, yet possible event that we require physical access to restore service.

Given the widespread nature of this threat, we have already begun preparing by downloading the necessary Microsoft updates to our client servers, as downloading the updates does not require downtime and will optimize our efficiency.

Further information regarding this vulnerability is available on Microsoft's website at the following link:

[HAFNIUM targeting Exchange Servers with 0-day exploits - Microsoft Security](#)

Aaron Arlotti
Manager, Remote Support Operations
Sandbox Technologies, Inc

Copyright © 2021, Sandbox Technologies, Inc. All rights reserved.

Our mailing address is:

4111 West Alameda Ave., Suite 605 Burbank, CA 91505

Want to change how you receive these emails?

To request an address change or to unsubscribe from this list, reply with the word "UNSUBSCRIBE" in the subject, or send an email to subscriptions@sandboxtech.com .