MARCH 18, 2021

Alert: Hafnium Cyber Attacks

IMMEDIATE INTELLIGENCE & ACTIONABLE GUIDANCE

Nation-state actors often leverage the effects of cyber operations to achieve their strategic objectives on the world's stage.

WHAT OCCURRED?

A nation-state threat group known as 'Hafnium' is targeting entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

The Cybersecurity and Infrastructure Security Agency (CISA) released an emergency directive regarding this targeted attack, which includes background information and required actions. View the alert here.

WHAT IS THE IMPACT?

Hafnium is exploiting vulnerabilities to compromise the Microsoft Exchange platform and all data (email primarily) within. A cyber actor would be able to use the access to potentially facilitate wider compromise of an organization's network.

Attacks have been ongoing since at least January 2021, and CISA recommends looking for signs of compromise from as far back as September 1, 2020, if not further. Microsoft released an out-of-band update to fix the critical vulnerabilities and posts new information regarding security updates and response steps here.

The availability of these updates makes it likely that attacks using the same vulnerabilities will be conducted by less capable groups. CISA reported that cyber actors are searching for these vulnerabilities using open source tools.

WHO IS IMPACTED?

Organizations with on premises Microsoft Exchange (2013, 2016, or 2019) either exclusively or in a hybrid model with cloud infrastructure. Organizations exclusively using Microsoft 365 hosted email or another email platform are not affected. Exchange Online is not affected.

IMMEDIATE RECOMMENDATIONS

- If evidence of compromise is discovered, begin forensic analysis, primarily focusing on artifact collection and data preservation.
- Ensure your organization applies the latest patches, available here.
- If unable to apply updates immediately, alternative mitigation options can be found here.
- Ensure the antivirus and intrusion detection solution deployed has detections in place for the indicators of compromise.
- Conduct threat hunting searches against your Exchange infrastructure to determine if any components have artifacts associated with this incident. Common initial post exploitation activity is the installation of an aspx web shell followed by further compromise including the extraction of Active Directory credentials. Examples of these artifacts can be found here.
- If your organization is using Splunk, then further information can be found here.
- Organizations should review the Indicators of Compromise provided here against their Exchange instance.

ISSUED ADVISORIES

- Microsoft Releases Exchange On-premises Mitigation Tool
- Updates on Microsoft Exchange Server Vulnerabilities
- CISA Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
- CISA Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities
- NCSC Alert: Advice Following Microsoft Vulnerabilities Exploitation

National Cyber Security Centre
a part of GCHQ

How FTI Cybersecurity Can Help

A global team of cybersecurity experts with extensive experience hunting, identifying, and responding to advanced persistent threat (APT) actors at government and private organization. Our team, capable of deploying worldwide, consists of dedicated cybersecurity experts, incident response consultants, developers, and data scientists with extensive investigative backgrounds. With our global team's deep experience in intelligence, law enforcement, and senior levels of government, **we maintain relationships with the top global intelligence agencies, regulatory authorities, and private agencies** to better support our clients in their prevention, response, and investigation of cyber threats and incidents. We can help by:

- **Understanding and assessing potential impact to your organization:** Analysis of systems and networks to determine if a breach occurred, and if so, what was affected and how to properly proceed.
- **Independent expert investigative task force:** Rapid response and surge capabilities anywhere in the world, capable of unearthing key facts and data sets.
- **Incident response:** Assist with containment, eradication, and recovery, including prohibiting data from leaving networks and preventing further damage.
- **Reviewing and assessing network architecture:** Audit of various network aspects in order to identify potential weaknesses in existing network configurations or changes to those configurations that may pose a risk to the organization.
- **APT threat-hunting services:** Ensure that the indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with this threat do not exist within your network. This service offering will focus on the following areas:
  - User authentication events analysis to ensure only expected events exists.
  - Host-based threat hunting for IOCs associated with this event.
  - Network threat hunting for the network IOCs associated with this event.
- **Holistic cybersecurity program assessment:** Ensure that existing policies and procedures are in place to handle an incident of this nature.

ANTHONY J. FERRANTE
Senior Managing Director
Global Head of Cybersecurity
ajf@fticonsulting.com

JORDAN RAE KELLY
Senior Managing Director
Head of Cybersecurity, Americas
jordan.kelly@fticonsulting.com

KYUNG KIM
Senior Managing Director
Head of Cybersecurity, APAC
kyung.kim@fticonsulting.com

JOSHUA BURCH
Senior Managing Director
Head of Cybersecurity, EMEIA
joshua.burch@fticonsulting.com