



# HAFNIUM (HF) ATTACK

Microsoft Exchange or  
Microsoft Ex-change

Happiest Minds' Cyber Security Incident Response Team (CSIRT) was involved in firsthand incident analysis and response preparation. In this exercise, we have observed a few unique attack characteristics, which are detailed below:

## PREREQUISITES

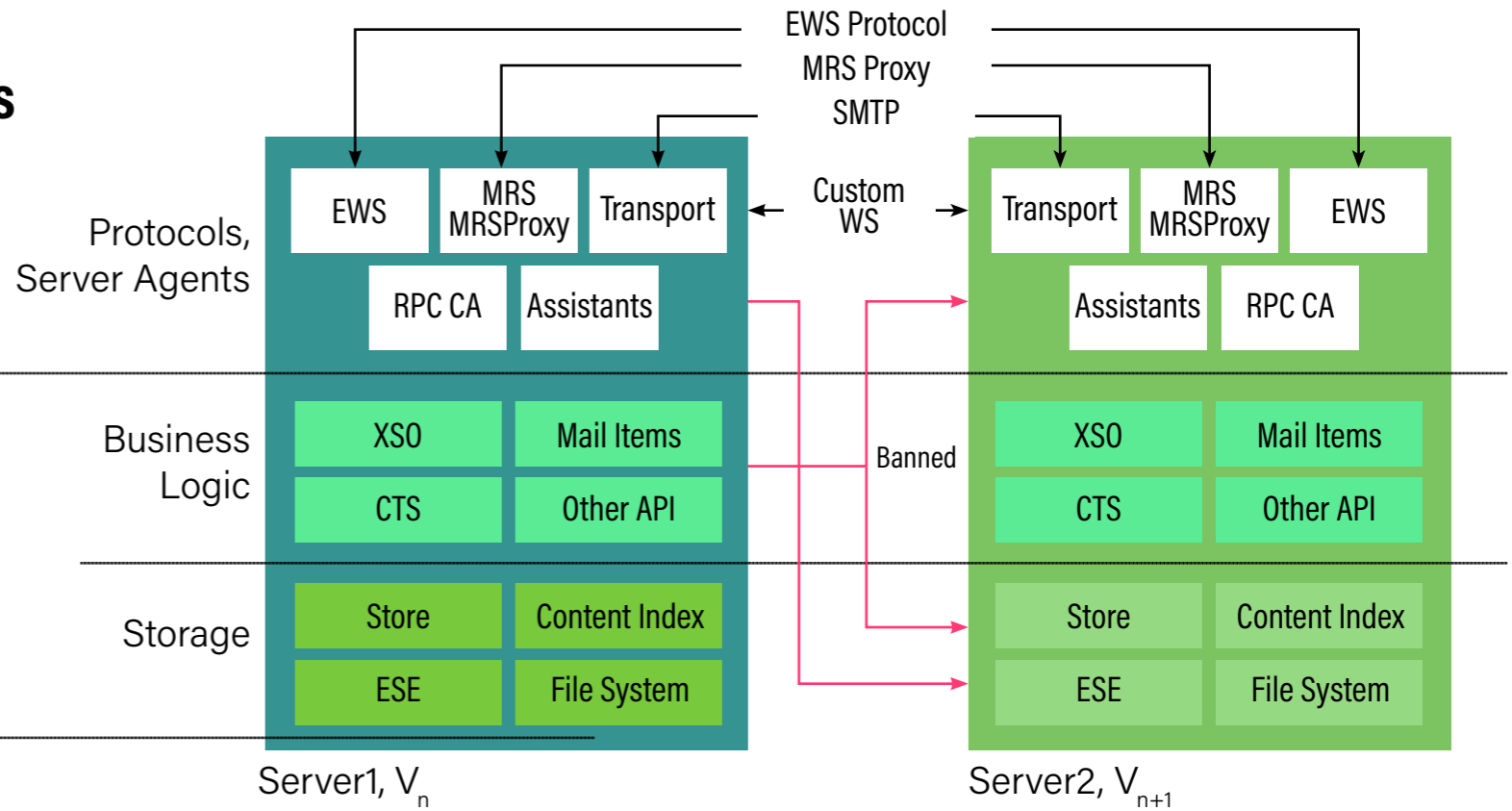
Understanding of key building blocks in Exchange 2013 and onwards

### Client Access Server (CAS) functions

- Authentication
- Proxying
- Redirection
- Load Balancing

### MBX Functions

- Biz logics
- Storage



Attackers group named 'Hafnium,' unlike the likely reason of their name, a completely non-toxic chemical Hafnium (Hf) [Atomic# 72], has rippled the cyber world by exploiting Microsoft's Exchange, a flagship enterprise emailing platform.

The attack has jolted the cyber world, especially Exchange on-premises deployment, which is used globally by ~350 Million mailboxes.

1

Authentication can be through local or through a central directory like AD. This functionality authenticates any client who intends to connect to Exchange

2

Proxying is the CAS functionality which renders backend services even if the clients connect through Web, POP, IMAP or server-side connections on SMTP or any UC services

# ATTACKER ACTIONS

## Exploited Server-Side Request Forgery (SSRF) vulnerability on Exchange servers

### WHAT

A weakness in the webserver which lets an attacker use the web server as a web client (like chrome, IE, Mozilla Firefox, Safari, and others) but with a command line.

### HOW

Attackers made random HTTP POST requests on Exchange servers which had CAS exposing HTTP proxy to render Outlook Web Access (OWA). The HTTP POSTs were targeting valid style sheets, gif files on Exchange servers at the path `/owa/auth/Current/themes/resources/<<xxx>>.css`.



Exchange servers were vulnerable, and such POST requests bypassed authentication and granted 'LOCAL ADMIN/SYSTEM' rights to the attacker.

## ATTACKER ACTIONS

With SYSTEM access, the attackers placed 'Web Shell' on the compromised server. These 'Web Shells' were named with common names like 'Login.aspx,' which could easily go unnoticed during investigations

### WHAT

A Web shell is a script written in common web languages like ASP, Python, Ruby and others, which gives the attacker a command line to use the server as a client to run web requests of attackers' choice (SSRF).

### HOW

The most used shell by the attackers was a well-known shell, 'China Chopper'. This shell is meagerly 2-3KB in size, and an attacker could literally type and build the shell on the server without needing any file to be transferred over a network.



## ATTACKER ACTIONS

### Now it's 'Nirvana'

#### WHAT

Attacker with system-level privileges on the server and 'Web Shell' implanted to execute under same permission levels

#### HOW

Hafnium used this to access all mailboxes, scoop away sensitive information, get access to the local directory server, escalate privileges in a network and keep moving laterally inside the network.



## EXPLOITED VULNERABILITIES



### CVE-2021-26855

---


This is a server-side request forgery (SSRF) vulnerability in Exchange, which enabled the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.



### CVE-2021-26857

---

This is an insecure deserialization vulnerability in the Unified Messaging service. It is where a program deserializes untrusted user-controllable data. Exploiting this vulnerability provided HAFNIUM with the ability to run code as a SYSTEM on the Exchange server. This needs the permission of an administrator or another vulnerability to exploit.



### CVE-2021-26858

---

This is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM can authenticate with the Exchange server, then they could easily use this vulnerability to write a file to any path on the server. This allows them to authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.



### CVE-2021-27065

---

This is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM can authenticate with the Exchange server, then they could use this vulnerability to write a file to any path on the server. This allows them to authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

## FROM CISO'S DESK



**VIJAY BHARTI**  
SVP, Head of CSIRT,  
Happiest Minds Technologies

This again is a stark reminder of how vulnerable IT systems are. It is just a matter of time; another "Zero-day" vulnerability is found and exploited to cause havoc on businesses. Organizations need to prepare for such eventualities by -



Design systems for minimum impact by leveraging least privileges, Zero Trust architectures



Invest in advanced Detective controls and mechanism for faster detection, analysis, and response



Continuously test/review, conduct Cyber drills and exercises to ensure a coordinated response



Happiest Minds Technologies

# Your Cyber Security Partner!

Happiest Minds with its presence in India, U.S., UK, Canada, Australia and Middle East countries has very niche Cyber Security Incident Response Team (CSIRT) helping customers in solutioning advance detection techniques. CSIRT is vendor agnostic team with top notch Infosec practitioners working directly under supervision of CISO of Happiest Minds, Mr Bharti.

## Key services from CSIRT

- 1 Preparing customers for better incident handling
- 2 Consulting customers to shift from negative incident handling models to positive models
- 3 Consult customers add 'Visibility' with measurable KPIs in the infosec program

If you are impacted/attacked, please email us at  
**[business@happiestminds.com](mailto:business@happiestminds.com)**  
for a pro-bono log analysis and plan the next steps.

[www.happiestminds.com](http://www.happiestminds.com)

 happiest minds  
The Mindful IT Company  
Born Digital . Born Agile