kindred

Security Newsletter

8 March 2021

Subscribe to this newsletter

4 Actively Exploited 0-Day Flaws Found in Microsoft Exchange

Microsoft has released emergency patches to address four previously undisclosed security flaws in Exchange Server that it says are being actively exploited by a new Chinese state-sponsored threat actor with the goal of perpetrating data theft.

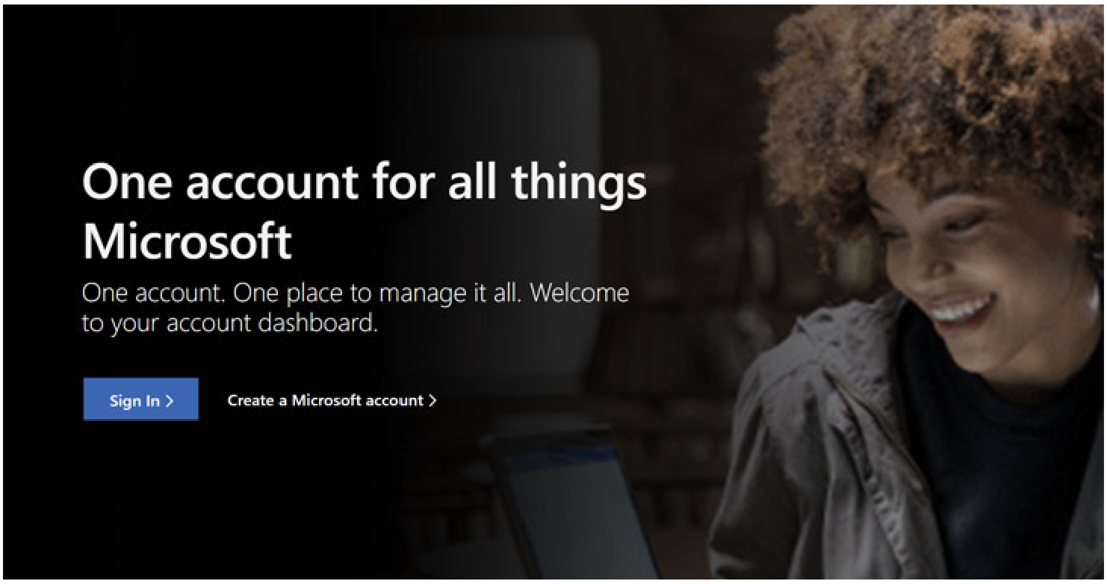
The tech giant primarily attributed the campaign with high confidence to a threat actor it calls HAFNIUM, a state-sponsored hacker collective operating out of China, although it suspects other groups may also be involved.

A successful exploitation of the flaws allows the adversaries to break into Microsoft Exchange Servers in target environments and subsequently allow the installation of unauthorized web-based backdoors to facilitate long-term access.

Read More on TheHackerNews

Even More on Microsoft security blog

A $50,000 Bug Could've Allowed Hackers Access Any Microsoft Account



One account for all things Microsoft

One account. One place to manage it all. Welcome to your account dashboard.

Microsoft has awarded an independent security researcher $50,000 as part of its bug bounty program for reporting a flaw that could have allowed a malicious actor to hijack users' accounts without their knowledge.

Reported by Laxman Muthiyah, the vulnerability aims to brute-force the seven-digit security code that's sent to a user's email address or mobile number to corroborate his (or her) identity before resetting the password in order to recover access to the account.

The company addressed the issue in November 2020, before details of the flaw came to light on Tuesday.

Read More on TheHackerNews

More #News

- Okta to Buy Auth0 for $6.5 Billion
- At Least 30,000 U.S. organizations hacked via Exchange 0-days
- Quality, not quantity, is the hallmark of the latest waves of phishing attacks
- I see you: your home-working photos reveal more than you think!
- Ransomware gang plans to call victim's business partners about attacks

#Breach Log

- Airlines warn passengers of data breach after aviation tech supplier is hit by cyberattack
- Accellion zero-day claims a new victim in cybersecurity company Qualys
- Three Top Russian Cybercrime Forums Hacked
- Accellion Appliance Zero-Day Attack Breaches: Key Takeaways
- Unpatched QNAP devices are being hacked to mine cryptocurrency

#Patch Time!

- Another Chrome zero-day exploit – so get that update done!
- Protecting against recently disclosed Microsoft Exchange Server vulnerabilities
- pppd vulnerable to buffer overflow due to a flaw in EAP packet processing
- VMware releases fix for severe View Planner RCE vulnerability
- Microsoft Exchange Server Vulnerabilities Mitigations

#Tech and #Tools

- Microsoft Defender for Identity: AS-REP Roasting
- Side Channel Attacks on the CPU On-Chip Ring Interconnect Are Practical
- Spotting the Red Team on VirusTotal!
- Microsoft's MSERT tool now finds web shells from Exchange Server attacks
- CertWatcher — Automating Certificate Transparency OSINT with Apps Script
- No, RSA Is Not Broken
- Wubes: Leveraging the Windows 10 Sandbox for Arbitrary Processes

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us