HC3: Alert

November 17, 2021 TLP: White Report: 202111171300

Joint CISA/FBI/ACSC/NCSC Alert - Iranian Government APTs Exploiting Microsoft Exchange via Fortinet Vulnerabilities

Executive Summary

The Cybersecurity & Infrastructure Security Agency (CISA, part of the Department of Homeland Security) along with the Federal Bureau of Investigation (FBI), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) warned of an Iranian government-sponsored advanced persistent threat (APT) exploiting Fortinet vulnerabilities and a Microsoft Exchange ProxyShell vulnerability to gain access to systems to launch cyberattacks, including the deployment of ransomware.

Report

Alert (AA21-321A) Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities
https://us-cert.cisa.gov/ncas/alerts/aa21-321a

Impact to HPH Sector

The US, UK, and Australian agencies collectively warned that they've observed this Iranian APT exploit Fortinet vulnerabilities since at least March 2021, and a Microsoft Exchange ProxyShell vulnerability since at least October 2021. Ransomware is a consistent threat to the health sector. Furthermore, these technologies – Microsoft Exchange and Fortinet FortiOS – are known to be leveraged by the health sector. All Healthcare and Public Health entities are encouraged to review the report to determine potential impact to their infrastructure and follow the countermeasure, mitigation, and patching instructions accordingly.

References

US, UK warn of Iranian hackers exploiting Microsoft Exchange, Fortinet
https://www.bleepingcomputer.com/news/security/us-uk-warn-of-iranian-hackers-exploiting-microsoft-exchange-fortinet/

Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities
https://www.cyber.gov.au/acsc/view-all-content/advisories/iranian-government-sponsored-apt-cyber-actors-exploiting-microsoft-exchange-and-fortinet-vulnerabilities-furtherance-malicious-activities

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback