PRESS RELEASE | Sept. 14, 2022

Iranian Cyber Actors Exploit Known Vulnerabilities to Extort U.S. Critical Infrastructure Organizations, Other Victims

In a Cybersecurity Advisory released today, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), NSA, U.S. Cyber Command, the Department of Treasury and international partners reveal how Iranian cyber actors continue to exploit known vulnerabilities on unprotected networks to extort and ransom victims, including U.S. critical infrastructure organizations.

In "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disc Encryption for Ransom Operations," agencies from four nations provide specific examples of IRGC-affiliated cyber actors exploiting Fortinet, Microsoft Exchange and VMware Horizon log4j vulnerabilities to gain initial access to systems. The actors then leveraged the access for disk

Skip to main content (Press Enter).

encryption and data extortion to support ransom operations.

The advisory release is part of a U.S. Government effort to eradicate this malicious activity and hold the IRGC-affiliated actors responsible. The malicious actors are actively targeting a broad range of victims, including entities across multiple U.S. critical infrastructure sectors as well as Australian, Canadian and United Kingdom organizations. The Cybersecurity Advisory provides tactics, techniques and procedures and indicators of compromise.

NSA and its partners recommend that organizations, especially those with ties to critical infrastructure networks, use the guidance to mitigate risk of compromise. A patch has been released for each vulnerability identified in the advisory and the most effective mitigation is to patch and update operating systems, software and firmware.

The agencies also recommend that organizations using Microsoft Exchange servers, Fortinet devices and/or VMware Horizon investigate suspicious activity in their networks using the detection guidance in the advisory.

Read the full report here.

Visit our full library for more cybersecurity information and technical guidance.


SHARE


PRINT

Related Press Advisories

NSA, CISA, and FBI Expose PRC State-Sponsored Exploitation of Network Providers, Devices

NSA, Partners Recommend Properly Configuring, Monitoring PowerShell in New Report

PowerShell in New Report

NSA Publishes Guidance on Characterizing Threats, Risks to DoD Microelectronics

NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers

cybersecurity iran irgc Iranian Islamic Revolutionary Guard Corps FBI CISA NCSC ACSC Fortinet VMware horizon log4j vulnerability microsoft exchange ransomware extortion