UK and allies expose Iranian state agency for exploiting cyber vulnerabilities for ransomware operations

Joint advisory highlights threat from cyber actors affiliated with Iran's IRGC.

The UK and international allies have issued a joint cyber security advisory highlighting that cyber actors affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC) are exploiting vulnerabilities to launch ransomware operations against multiple sectors.

Iranian-state APT actors have been observed actively targeting known vulnerabilities on unprotected networks, including in critical national infrastructure (CNI) organisations.

The advisory, published by the National Cyber Security Centre (NCSC) - a part of GCHQ - alongside agencies from the US, Australia and Canada, sets out tactics and techniques used by the actors, as well as steps for organisations to take to mitigate the risk of compromise.

It updates an advisory issued in November 2021 which provided information about Iranian APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities.

They are now assessed to be affiliated to the IRGC and are continuing to exploit these vulnerabilities, as well as the Log4j vulnerabilities, to provide them with initial access, leading to further malicious activity including data extortion and disk encryption.

Paul Chichester, NCSC Director of Operations, said:

> "This malicious activity by actors affiliated with Iran's IRGC poses an ongoing threat and we are united with our international partners in calling it out.
>
> "We urge UK organisations to take this threat seriously and follow the advisory's recommendations to mitigate the risk of compromise."

The NCSC urges organisations to follow the mitigation set out in the advisory, including:

- Keeping systems and software updated and prioritising remediating known exploited vulnerabilities
- Enforcing multi-factor authentication
- Making offline backups of your data

This advisory has been issued by the NCSC, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), US Cyber Command (USCC), Department of the Treasury (DoT), the Australian Cyber Security Centre (ACSC) and the Canadian Centre for Cybersecurity (CCCS).

Read the advisory in full on the CISA website

PUBLISHED

20 September 2022

WRITTEN FOR

Small & medium sized organisations

Large organisations

Cyber security professionals

NEWS TYPE

General news