UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00131

FORTINET FLAW RANSOMWARE ATTACK

DATE ISSUED: 12th April 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

A new ransomware strain known as Cring has burst onto the scene in a recent attack targeting industrial Enterprises via a flaw in Fortinet's FortiOS. CVE-2018-13379

BREAKDOWN

Attacks have been recorded across Europe thus far with this unique new ransomware capable of forcing a shutdown of industrial processes. The attackers exploited a path-reversal flaw present in unpatched versions of FortiOS to deliver the Cring ransomware which uses destroys backups and uses two kinds of encryption to prevent the restoration of files. Tied to the system's SSL VPN Web Portal, the flaw allows an attacker to access and download system files without the need for authentication, using bespoke HTTP resource requests. The attack chain commences with a directory-traversal attack (CVE-2018-13379) to access vulnerable hardware providing access to network credentials and establish a persistent threat on the targeted network and access the system files of FortiOS, connecting using 'sslvpn_websession,'where the username and passwords are stored in plaintext.

REMEDIATION STEPS

- Install patches immediately to any affected devices.
- Isolate devices from the network that are unable to be patched.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/hackers-exploit-flaw-cring-ransomware/165300/
Kaspersky https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/
SC Magazine https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/