December 2020

WEEKLY CYBER THREAT LEVEL INDICATOR

SEVERE RISK

Indicators:
Red - Severe
Orange - High
Yellow - Elevated
Blue - Guarded
Green - Low

HAWKEYE
HUNTING CYBER ADVERSARIES

HAWKEYE WEEKLY ROUNDUP

CYBER THREAT LANDSCAPE

WHAT'S TRENDING?

Sunburst's C2 Secrets Reveal Second-Stage SolarWinds Victims

More information has come to light about the Sunburst backdoor that could help defenders get a better handle on the scope of the sprawling SolarWinds espionage attack.

Cloud is King: 9 Software Security Trends to Watch in 2021

Researchers predict software security will continue to struggle to keep up with cloud and IoT in the new year. IT security professionals have largely spent the year managing a once-in-a-generation workforce shift from office to home in 2020.

Microsoft Caught Up in SolarWinds Spy Effort, Joining Federal Agencies

Microsoft has become the latest victim of the ever-widening SolarWinds-driven cyberattack that has impacted rafts of federal agencies and tech targets.

Nuclear Weapons Agency Hacked in Widening Cyberattack

The Energy Department and its National Nuclear Security Administration (NNSA), which is the agency that maintains the U.S. nuclear stockpile, have been compromised as part of the widespread cyberattack uncovered this week stemming from the massive SolarWinds hack.

CRITICAL VULNERABILITIES

CVE

5M WordPress Sites Running 'Contact Form 7' Plugin Open to Attack

The critical vulnerability (CVE-2020-35489) is classified as an unrestricted file upload bug, according to Astra Security Research, which found the flaw on Wednesday.

Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome

The Firefox and Chrome bug in question (CVE-2020-16042) is still not fully described by either browser maker, and is only listed as a memory bug.

ICS Advisory (ICSA-20-352-01) Emerson Rosemount X-STREAM

CVSS v3 7.5

Successful exploitation of this vulnerability could allow an attacker through a specially crafted URL to download files and obtain sensitive information.

ICS Advisory (ICSA-20-353-01) Treck TCP/IP Stack

CVSS v3 9.8

Successful exploitation of this vulnerability may allow remote code execution and a denial-of-service condition.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Palo Alto Networks CEO: All Companies Must Ensure They Weren't Hit in Suspected Russian Cyberattack

Palo Alto Networks CEO Nikesh Arora told CNBC on Friday that every business and federal agency needs to take stock of their network security in the wake of the suspected Russian massive cyberattack.

Fortinet Ensures Secure Cloud Migration for European Real Estate Company

In our digital world, individuals increasingly rely on continued connectivity for work, learning, and entertainment. Because of this, organizations face unique security challenges as they try to secure both their employees leveraging business critical applications and customers accessing their Wi-Fi networks from personal devices.

FireEye Hit by Possible Nation-State Cyberattack

American cybersecurity firm FireEye has suffered a data breach, which it has described as unprecedented. Announcing the news in a blog post, the company said the attack was perpetrated by a "highly sophisticated threat actor" – most likely a state-sponsored group. They managed to steal the company's tool used for testing customer security, most likely going after customers from the public sector.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

How to Increase Your Security Posture with Fewer Resources

With security teams limited in resources, especially as state and public schools and universities are facing shortages caused by the coronavirus, educational institutions and others must find a way to increase their security posture to reduce threats like ransomware from taking hold.

12 Ways to Defeat Multi-Factor Authentication

Everyone knows that multi-factor authentication (MFA) is more secure than a simple login name and password, but too many people think that MFA is a perfect, unhackable solution. It isn't! How to better defend your MFA solution so that you get maximum benefit and security.

3 million Downloaded These Malicious Extensions. Did You?

More than three million internet users are believed to have installed 15 Chrome, and 13 Edge extensions that contain malicious code, according to security firm Avast. The 28 extensions contained code that could perform several malicious operations.
Avast researchers said they believe the primary objective of this campaign was to hijack user traffic for monetary gains.

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

ABU DHABI | KUWAIT CITY | YEREVAN | LONDON
www.dts-solution.com

800 HACKED