24 November 2021

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?

Threats to ICS and Industrial Enterprises in 2022

Improved corporate cybersecurity and the introduction of ever more tools and protection measures are causing cyberthreats to evolve.

Human-based Risks are the Biggest Threat to Your Organization

Regardless of their intent, individuals create risk every day for your business — while simply doing their jobs. In fact, research finds 83% of organizations experienced a serious incident caused by human error. The 2021 Egress Insider Data Breach Survey also finds 73% of enterprises have been victims of phishing.

Common Cloud Misconfigurations Exploited in Minutes, Report

Poorly configured cloud services can be exploit by threat actors in minutes and sometimes in under 30 seconds. Attacks include network intrusion, data theft and ransomware infections, researchers have found.

US Govt Warns Critical Infrastructure of Ransomware Attacks During Holidays

US CISA and the FBI issued a joint alert to warn critical infrastructure partners and public/private organizations of ransomware attacks during holidays. The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI warn critical infrastructure partners of ransomware attacks during the holiday season.

CRITICAL VULNERABILITIES

CVE

New GoDaddy Data Breach Impacted 1.2 Million Customers

GoDaddy discloses a data breach that impacted up to 1.2 million of its customers, threat actors breached the company's Managed WordPress hosting environment. Threat actors compromised the company network since at least September 6, 2021, but the security breach was only discovered by the company on November 17.

Microsoft Informs Users of High-Severity Vulnerability in Azure AD

Tracked as CVE-2021-42306 (CVSS score of 8.1), the vulnerability exists because of the manner in which Automation Account "Run as" credentials are created when a new Automation Account is set up in Azure.

Expert Released PoC Exploit Code for Microsoft Exchange CVE-2021-42321 RCE Bug

The CVE-2021-42321 is a high-severity remote code execution issue that occurs due to improper validation of cmdlet arguments. Microsoft pointed out that the flaw can be exploited only by an authenticated attacker.

Experts Warn of RCE Flaw in Imunify360 Security Platform

Cisco's Talos researchers discovered a remote code execution vulnerability, tracked as CVE-2021-21956, in CloudLinux's Imunify360 security product. The flaw resides in the Ai-Bolit functionality of CloudLinux Inc Imunify360 and an attacker could exploit it to execute arbitrary code using specially crafted files.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Cisco Partners with JupiterOne to Enhance Its SecureX Product Portfolio

Cisco announced this week it has partnered with cloud security and governance platform provider JupiterOne to launch Cisco Secure Cloud Insights. Secure Cloud Insights will be part of Cisco's SecureX family of products and is intended to help customers manage risk and reduce the attack surface of their cloud-based processes and applications.

Cyware Partners with Flashpoint to Empower Security Teams to Automate Threat Response Workflows

Cyware announced an expanded partnership with Flashpoint to deliver intelligent automation to security teams. The partnership now features a solution that enables customers to leverage Flashpoint's intelligence data with Cyware's Security Orchestration Layer (CSOL), providing the advanced workflow automation necessary to help security analysts build more efficiency into threat response.

Alkira Partners with Exclusive Networks to Expand Its Cloud Market share

Alkira has appointed Exclusive Networks, a global trusted cybersecurity specialist for digital infrastructure, as a distributor for its cloud networking as-a-service platform (CNaaS).

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

How to Strengthen Incident Response in the Health Sector

Cybersecurity attacks on healthcare may also affect the entire health supply chain with damaging consequences for all stakeholders concerned such as citizens, public authorities, regulators, professional associations, industries, small and medium enterprises.

How to Handle Third-Party Security Risk Management

In today's hyper-connected world, organizations are highly dependent on third-party vendors to efficiently run their business. Therefore, it is crucial to efficiently and effectively manage third-party security risk in your company.

Zero Trust: An Answer to the Ransomware Menace?

Zero trust helps to minimize the lateral movement of attackers (i.e., techniques used by intruders to scout networks) through the principle of "never trust, always verify."

5 Predictions to Help you Focus Your Web App Security Resources in 2022

The past year in web app cybersecurity was anything but calm, and if predictions on the coming year from PerimeterX CTO are accurate, it's going to be another year of struggles to protect web apps.

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