01 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?

Why the Next-Generation of Application Security Is Needed

Software is revolutionizing the way the world operates. From driverless cars to cryptocurrency, software reimagines possibilities. With software standing at the core of everything we do, we find ourselves pushing out code faster than ever. Current estimates show that there are more than 111 billion lines of new code written per year. New software and code stand at the core of everything we do, but how well is all of this new code tested? Luckily, autonomous application security is here.

Software Composition Analysis Mitigates Systemic Risk in the Popular NPM Repository

The attackers modified the library to include password stealers and crypto miners so that the applications of anyone who downloaded that version would be compromised. With an attack like this, the applications that are using this library with this code are going to be running that code with the privileges that they have, wherever they're deployed.

What Exactly Is Secure Access Service Edge (SASE)?

The hybrid work environment is here to stay. People will continue to work from home some days, use devices that are both personally owned and corporate-issued, and use apps that reside in the cloud. While this level of flexibility has come to be what employees expect and has also increased productivity for organizations, it comes with an expansion of the attack surface and created increased complexity for IT, security, and networking teams.

CRITICAL VULNERABILITIES

CVE

Cisco Fixes an OS Command-Injection Flaw, Tracked as CVE-2021-1529, in Cisco SD-WAN that Could Allow Privilege Escalation and Lead to Arbitrary Code Execution

An authenticated, local attacker can exploit the CVE-2021-1529 vulnerability to execute arbitrary commands with root privileges. The CVE-2021-1529 received a CVSS score of 7.8.

Critical Flaw in GoCD Provides Platform for Supply Chain Attacks

A critical vulnerability in popular CI/CD tool GoCD could allow unauthenticated attackers to extract encrypted secrets and poison software build processes — potentially paving the way to supply chain attacks.

Misconfigured Database Leaks 880 Million Medical Records

Researchers have found an unsecured database leaking over 886 million patient records online, although it's now confirmed that this was dummy data.

Over 1 Million WordPress Sites Affected by OptinMonster Plugin Flaws

A high-severity vulnerability (CVE-2021-39341) in The OptinMonster plugin can allow unauthorized API access and sensitive information disclosure on roughly a million WordPress sites.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Imperva Snapshot Delivers Cloud Data Security Posture Assessment for Amazon RDS Managed Databases

Imperva introduces the Imperva Snapshot service, a free cloud data security posture assessment for Amazon Relational Database Service (Amazon RDS) managed databases. New patent-pending technology identifies infrastructure and database misconfigurations and performs vulnerability assessments and data classification through a data-aware technique, which does not rely solely on the available cloud vendor Application Programming Interfaces (APIs).

DTEX Systems Provides Insider Threat Intelligence and Investigation Services with DTEX I3 Research Team

DTEX Systems launched DTEX Insider Intelligence and Investigations (DTEX I3), an expanded investigations and research division focused on delivering insider threat behavioral studies, intelligence packages and forensic investigations.

Appgate Launches SDP Solution to Help Enterprises Expand and Accelerate Zero Trust Initiatives

Appgate released its Zero Trust Network Access (ZTNA) solution, introducing an array of capability and usability enhancements designed to help enterprises expand and accelerate strategic zero trust initiatives.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

OT Security: Risks, Challenges and Securing your Environment

Operational Technology is the combination of hardware and software that controls and operates the physical mechanisms of industry.

Enterprise Backups Are Becoming Targets for Cybercriminals

In ransomware attacks, cybercriminals attack through the backups because they know that security practitioners rely on backups to save themselves after a ransomware attack.

Three OT Security Lessons Learned from 2021's Biggest Cyber Incidents

What do an oil pipeline, a water treatment plant, and a railway system have in common? They each rely on operational technology (OT) environments, and they were all victims of cyber-attacks that generated headlines around the world.

How Do I Select an SD-WAN Solution for My Business?

SD-WAN adoption has also shifted from being mostly used by big organizations, to being considered by SMBs as well, who have realized the potentials and benefits of such technology.

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