

**WEEKLY
CYBER
THREAT
LEVEL
INDICATOR**
**SEVERE
RISK**

Indicators:

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


CYBER THREAT LANDSCAPE
WHAT'S TRENDING?
How to Use Bitwarden's New Send Feature

What is probably the best open source password manager on the market has added a new feature that will make using the tool even better.

ProxyLogon Microsoft Exchange Exploit Is Completely Out of the Bag by Now

A security researcher has released a new proof-of-concept exploit that could be adapted to install web shells on Microsoft Exchange servers vulnerable ProxyLogon issues. Since the disclosure of the flaw, security experts observed a surge in the attacks against Microsoft Exchange mailservers worldwide. Check Point Research team reported that that in a time span of 24 hours the exploitation attempts are doubling every two hours.

Cyberattacks See Fundamental Changes, A Year into COVID-19

A year after the COVID-19 crisis was officially determined to be a pandemic, the way people live and work has radically changed – and so have "the methods and tactics used by criminals on the internet looking to exploit the massive increase in online traffic," according to a report from Kaspersky


CYBER SECURITY NEWS
WHAT'S NEW FROM VENDORS?
Microsoft Releases One-Click Exchange On-Premises Mitigation Tool

Microsoft has released Exchange On-Premises Mitigation Tool (EOMT), which quickly performs the initial steps for mitigating the ProxyLogon flaw (CVE-2021-26855) on any Exchange server and attempts to remediate found compromises.

CoSoSys Updates Its Endpoint Protector, Focusing On Enterprise Security and Compliance

CoSoSys launched the latest update of its Endpoint Protector 5.3.0.0. The product update brings enterprise-grade security features and important enhancements of existing functions that help to protect data and prevent breaches more efficiently.

LoginID Raises \$6M to Accelerate Adoption of Passwordless Authentication

Siemens has mitigated 21 vulnerabilities in two of its virtualization software tools that, if exploited, could enable attackers to gain remote control, exfiltrate data or cause systems to crash. In a patch update, Siemens notes that the flaws, dubbed SSA-663999, are file parsing vulnerabilities that affect JT2Go, a 3D viewing tool, and Teamcenter, an enterprise visualization tool, in versions earlier than V13.1.0.1.


CRITICAL VULNERABILITIES
CVE
F5, CISA Warn of Critical BIG-IP and BIG-IQ RCE Bugs

F5 Networks is warning users to patch four critical remote command execution (RCE) flaws in its BIG-IP and BIG-IQ enterprise networking infrastructure. If exploited, the flaws could allow attackers to take full control over a vulnerable system.

Critical Security Hole Can Knock Smart Meters Offline

Critical security vulnerabilities in Schneider Electric smart meters could allow an attacker a path to remote code execution (RCE), or to reboot the meter causing a denial-of-service (DoS) condition on the device.

Netgear JGS516PE Ethernet Switch Flaws let Attackers Execute Remote Code

Netgear has published security updates to inscribe 15 severe vulnerabilities in its JGS516PE Ethernet switch. These flaws involve an unauthenticated remote code execution vulnerability which is considered as one of the critical flaws.

Microsoft Patch Tuesday Updates Fix 14 Critical Bugs

Microsoft has released its regularly scheduled March Patch Tuesday updates, which address 89 security vulnerabilities overall. Included in the slew are 14 critical flaws and 75 important-severity flaws.


SOMETHING TO THINK ABOUT
WHAT'S NEXT?
Power Equipment: A New Cybersecurity Frontier

As digital transformation continues to advance amid the COVID-19 pandemic and beyond, businesses must evaluate their security model to ensure they're prepared for the next normal. Power equipment must be part of the equation in an end-to-end cybersecurity strategy.

How Implementing Employee Monitoring Software Can Deliver Meaningful Returns

Gartner estimated that 80% of companies would implement some form of employee-monitoring software, a noteworthy 50% increase in five years.

The Importance of a Proactive Cyber Defense Solution To Protect Your Critical Data

This is the era of Cybercriminals and understanding their methods and means, is the most important factor to avoid becoming their next victim.

Cable Modems & Security

The newest malware is more sophisticated than its predecessors, which means that you also need to stay on top of it.