# *RED-N Managed Security*
## Weekly Update

*Week ending November 12, 2022*

## *Headline **NEWS***

- **Microsoft November 2022 Patch Tuesday** fixes 6 exploited zero-days, 68 flaws
- November 2022 **Security Update Review**
- **VMware** fixes **three critical auth bypass bugs** in remote access tool
- **Citrix** urges admins to **patch** critical **ADC, Gateway** auth bypass
- **Apple emergency code execution patch** released – but not a 0-day
- **Microsoft** fixes **ProxyNotShell Exchange zero-days** exploited in attacks
- **Lenovo** fixes **flaws** that can be used to disable **UEFI Secure Boot**
- **Paloalto Cortex XSOAR**: Local Privilege Escalation (**LPE**) Vulnerability
- Latest **Patch Tuesday** mends **Spectre V2 vulnerability** affecting **AMD Ryzen** Windows PCs
- **OpenSSL Vulnerabilities** Threat Brief: CVE-2022-3786, CVE-2022-3602 – good writeup
- **China** is likely **stockpiling** and deploying **vulnerabilities**, says Microsoft

## Other News Events of Note

- **Microsoft 365 Personal and Family** accounts to store email attachments, more, in OneDrive
- Analyzing **CISA Known Exploited Vulnerabilities** with Business Context - Security Boulevard
- **Microsoft** Digital Defense Report 2022 – Insights organizations need to defend themselves
- **CISA Warns** of Critical Vulnerabilities in 3 **Industrial Control** System Software
- **Medibank** says hacker accessed data of **9.7 million customers**, refuses to pay ransom
- A **cyberattack** blocked the **trains in Denmark**
- **LockBit** gang claims to have **stolen data** from **Kearney & Company**
- Opinion piece from Computer Weekly - **To fight ransomware**, we must **treat digital infrastructure as critical**
- **Maple Leaf Foods** suffers outage following weekend **cyberattack**
- The **HakCat WiFi Nugget** is a beginner’s guide to wireless mischief
- In another annoying idea, **Microsoft is showing ads** in the Windows 11 **sign-out menu**
- **SolarWinds** Faces Potential **SEC Enforcement** Action Over Orion Breach
- **Azov Ransomware** is a **wiper**, destroying data **666** bytes at a time
- **Cyberattack** disrupts **Mexico's transportation** system
- **Department of Justice** reveals massive **$3.36B crypto seizure**
- **Defense Department** Is Planning a **Secure Internet in Space**
- **McDonald's McCrispy Gaming Chair** Has a Fry Holder and Sandwich Warmer – sorry, UK only
- **Ransomware**, storage and **backup**: Impacts, limits and capabilities
- **Microsoft WinGet** package manager **failing** due to CDN issues
- **Microsoft** hits the switch on **password-free** smartphone **authentication**
- **Kaseya-Datto Shocker**: Rob Rae Has Left the Building
- **Microsoft's Certificate-Based Authentication** Enables Phishing-Resistant MFA
- Here's **what's new with Windows 11 22H2**'s first feature drop update
- **Abuse Microsoft** Dynamics 365 Customer **Voice** in **phishing** attacks
- **TCP/IP Vulnerability** CVE-2022–34718 PoC Restoration and Analysis
- **Malicious extension** lets attackers control **Google Chrome** remotely
- **Disabling Windows 11 security** settings gives a **major speed boost** to Intel GPUs
- The Easiest Way to **Simultaneously Record Your Screen and Webcam** on Windows
- **LockBit 3.0** Being Distributed via **Amadey Bot**
- Microsoft **.NET 7** is Now Available
- **15,000 sites hacked** for massive **Google SEO poisoning** campaign
- **Password**-based **hacks** have **increased 74%** over the last year
- Hackers are using a years-old **Microsoft SharePoint vulnerability** to attack governments around the world
- Over thirty **Arkansas counties** impacted by **cyber attack**
- **Taking down a ransomware hacker** – excellent reading
- Microsoft Exchange Online **Mail Flow Rules** Move to **New Exchange Admin Center**
- **Apple** Releases **iOS 16.1.1** and **iPadOS 16.1.1** With **Bug Fixes**
- **Google Pay** website **requiring 2FA** from December onwards
- **Cookies for MFA Bypass** Gain Traction Among **Cyberattackers**
- **TransUnion breached**, consumers' financial information exposed
- **Canadian** food retail giant **Sobeys** hit by **Black Basta ransomware**
- **Australian Government** announces team to **'hack the hackers'** after Medibank cyber attack
- At least **$1 billion** of client funds **missing** at **FTX**