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

Week ending December 24, 2022

*Headline **NEWS***

- Critical Windows code-execution vulnerability (CVE-2022-37958) went undetected until now
- MS Exchange CVE-2022-41040, CVE-2022-41082 – zero-days work-arounds defeated, being exploited, patch now
- Ransomware gang uses new Microsoft Exchange exploit (OWASSRF) to breach servers
- Microsoft Patch Tuesday for December 2022 — Snort rules and prominent vulnerabilities
- Microsoft: Patch Tuesday KB5021233 causing hidparse blue screen on Windows 10 22H2, more
- Microsoft pushes emergency fix for Windows Server Hyper-V VM issues
- Microsoft confirms it has fixed Direct Access connection issues on Windows 11, Windows 10
- Microsoft will turn off Exchange Online basic auth in January
- FBI Advises Consumers To Use Ad-Blockers
- The LastPass security incident keeps getting worse
- Comcast Xfinity accounts hacked in widespread 2FA bypass attacks
- Critical Security Flaw Reported in Passwordstate Enterprise Password Manager
- Puckungfu: A NETGEAR WAN Command Injection – upgrade your RAX30 firmware if lower than 1.0.9.90

Other News Events of Note

- NSA Publishes 2022 Cybersecurity Year in Review
- Microsoft: No optional Windows Updates this month due to holidays
- Stolen certificates in two waves of ransomware and wiper attacks
- Edison, NJ, Woman Among 6 Charged In Multi-Million Dollar Technical Support Scam Targeting 20,000 Victims
- FBI warns that BEC attacks now also target food shipments
- Digging into the numbers one year after Log4Shell
- Social Blade confirms breach after hacker posts stolen user data
- Some Medicare enrollees getting new ID numbers due to data breach
- Malicious ‘SentinelOne’ PyPI package steals data from developers
- New Agenda Ransomware Variant, Written in Rust, Aiming at Critical Infrastructure
- CFOs learn how to respond and lead during a cyberattack
- Colombian energy supplier EPM hit by BlackCat ransomware attack
- Glupteba Botnet Continues to Thrive Despite Google's Attempts to Disrupt It
- McGraw Hill's S3 buckets exposed 100,000 students' grades and personal info
- Microsoft finds macOS bug that lets malware bypass security checks
- Old vulnerabilities in Cisco products actively exploited in the wild
- Raspberry Robin Malware Targets Telecom, Governments
- Coming soon - Exchange Online Stops Remote PowerShell Connections
- FBI warns of explosion in sextortion cases targeting teenagers
- Ransomware in Higher Education: Holding My College Legacy Ransom
- CMS subcontractor hit with ransomware
- Malware Analysis: GuLoader Dissection Reveals New Anti-Analysis Techniques and Code Injection Redundancy
- Russia’s Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine
- GeForce Security Update Driver | 474.14 | Windows 10 64-bit, Windows 11 – security fixes
- Okta says source code for Workforce Identity Cloud service was copied
- Oops. Cisco installed wrong firmware on some boxes and they report fake ‘severe faults’
- Proxmox VE: Virtualization alternative to VMware ESXi and Hyper-V
- “Suspicious login” scammers up their game – take care at Christmas
- Mozilla Just Fixed an 18-Year-Old Firefox Bug
- Being one of the 1% sucks if you're a Rackspace user
- Fin7 Unveiled: A deep dive into notorious cybercrime gang
- Spam texts are out of control, say all 51 US attorneys general
- Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks
- Alternative to Microsoft’s long delayed LAPS for cloud joined devices - CloudLAPS Community Edition
- Shoemaker Ecco leaks almost 60GB of customer data