NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Bi-Weekly Cybersecurity Rollup

September 30, 2024

Included In This Summary

Click on the *section header* to go directly to that location in the summary.

Sensitivity/ Handling Notice:

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

NORTH DAKOTA AND REGIONAL

DSU receives $1 Million SBA Grant for Small Business Cybersecurity
Source: https://www.dakotanewsnow.com/2024/09/28/dsu-receives-1-million-sba-grant-small-business-cybersecurity/

NATIONAL

US-Led Operation Disrupts Crypto Exchanges Linked to Russian Cybercrime
Source: https://therecord.media/cryptocurrency-exchanges-seizures-ivanov-sanctions-us-netherlands

After TikTok Inquiry Republicans Call for Investigation into Temu Data Practices
Source: https://therecord.media/republicans-call-to-investigate-temu-china-tiktok

US Proposes Ban on Connected Vehicle Tech from China Russia
Source: https://www.bleepingcomputer.com/news/security/us-proposes-ban-on-connected-vehicle-tech-from-china-russia/

Exclusive: State Department Cyber Bureau Preps Funding Blitz Aimed at Boosting Allies' Defenses
Source: https://therecord.media/state-dept-preps-funding-blitz-to-boost-cyber-defenses-fick

Federal Civil Rights Watchdog Sounds Alarm Over DOJ DHS and HUD Use of Facial Recognition Technology
Source: https://therecord.media/federal-civil-rights-watchdog-facial-recognition-technology-report

DOJ Indicts Chinese National for Spearphishing Campaign Against NASA FAA Air Force
Source: https://therecord.media/doj-indicts-chinese-nationa-nasa-data-theft-aviation

THREATS / MALWARE

Hackers Deploy AI-written Malware in Targeted Attacks
Source: https://www.bleepingcomputer.com/news/security/hackers-deploy-ai-written-malware-in-targeted-attacks/

Compromised Credentials: New Cyberattack Exploits Industry Email Accounts
Source: https://securityonline.info/compromised-credentials-new-cyberattack-exploits-industry-email-accounts/

New Twist on Sextortion Scam Includes Pictures of People's Homes
Source: https://therecord.media/new-twist-on-sextortion-scam-pictures-of-peoples-homes

Dozens of Fortune 100 Companies Have Unwittingly Hired North Korean IT Workers According to Report
Source: https://therecord.media/major-us-companies-unwittingly-hire-north-korean-remote-it-workers

macOS Sequoia Change Breaks Networking for VPN Antivirus Software
Source: https://www.bleepingcomputer.com/news/apple/macos-sequoia-change-breaks-networking-for-vpn-antivirus-software/

Sensitivity/ Handling Notice:
Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Microsoft Entra ID's Administrative Units Weaponized to Gain Stealthy Persistence
Source: https://securityonline.info/stealthy-persistence-microsoft-entra-ids-administrative-units-weaponized/

Lumma Stealer Malware Campaign Exploits Fake CAPTCHA Pages
Source: https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages

Cybercriminals Exploit HTTP Headers for Credential Theft via Large-Scale Phishing Attacks
Source: https://thehackernews.com/2024/09/cybercriminals-exploit-http-headers-for.html

Malware Locks Browser in Kiosk Mode to Steal Google Credentials
Source: https://www.bleepingcomputer.com/news/security/malware-locks-browser-in-kiosk-mode-to-steal-google-credentials/

Multiple Attacks Forces CISA to Order Agencies to Upgrade or Remove End-of-Life Ivanti Appliance
Source: https://therecord.media/cisa-urges-federal-agencies-remove-ivanti-product

Targeted Campaigns in Retail Sector Involve Domain Fraud, Brand Impersonation, and Ponzi Schemes
Source: https://www.domaintools.com/resources/blog/retail-targeted-campaigns-domain-fraud-brand-impersonation-and-ponzi-schemes/

New Android Malware Ajina.Banker Steals 2FA Codes, Spreads via Telegram
Source: https://hackread.com/android-malware-ajina-banker-steal-2fa-codes-telegram/

VULNERABILITIES

Critical Ivanti vTM Auth Bypass Bug Now Exploited in Attacks
Source: https://www.bleepingcomputer.com/news/security/critical-ivanti-vtm-auth-bypass-bug-now-exploited-in-attacks/

WordPress Theme 'Houzez' and Associated Plugin Vulnerabilities Expose Thousands of Sites
Source: https://securityonline.info/wordpress-theme-houzez-and-associated-plugin-vulnerabilities-expose-thousands-of-sites/

Critical Flaw in Microchip ASF Exposes IoT Devices to Remote Code Execution Risk
Source: https://thehackernews.com/2024/09/critical-flaw-in-microchip-asf-exposes.html

Ivanti Warns of Another Critical CSA Flaw Exploited in Attacks
Source: https://www.bleepingcomputer.com/news/security/ivanti-warns-of-another-critical-csa-flaw-exploited-in-attacks/

CISA Warns of Actively Exploited Apache HugeGraph-Server Bug
Source: https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-apache-hugegraph-server-bug/

Patch this Critical Safeguard for Privileged Passwords Authentication Bypass Flaw
Source: https://www.helpnetsecurity.com/2024/09/19/cve-2024-45488/

Sensitivity/ Handling Notice:
Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Critical Grafana Plugin SDK Flaw Exposes Sensitive Information
Source: https://securityonline.info/cve-2024-8986-cvss-9-1-critical-grafana-plugin-sdk-flaw-exposes-sensitive-information/

CVE-2023-48788 Exploited: Researcher Details Cyberattacks on Fortinet FortiClient EMS
Source: https://securityonline.info/cve-2023-48788-exploited-researcher-details-cyberattacks-on-fortinet-ems/

Acronis Backup Plugins Hit by CVE-2024-8767: CVSS 9.9 Severity Alert
Source: https://securityonline.info/acronis-backup-plugins-hit-by-cve-2024-8767-cvss-9-9-severity-alert/

Zero-Click Calendar Invite: Critical macOS Vulnerability Chain Uncovered
Source: https://securityonline.info/zero-click-calendar-invite-critical-macos-vulnerability-chain-uncovered/

RANSOMWARE

New Mallox Ransomware Linux Variant Based on Leaked Kryptina Code
Source: https://www.bleepingcomputer.com/news/security/new-mallox-ransomware-linux-variant-based-on-leaked-kryptina-code/

Ransomware attack on Kansas County Exposed Sensitive info of Nearly 30000 Residents
Source: https://therecord.media/kansas-ransomware-attack-thousands-residents

Ransomware Gangs Now Abuse Microsoft Azure Tool for Data Theft
Source: https://www.bleepingcomputer.com/news/security/ransomware-gangs-now-abuse-microsoft-azure-tool-for-data-theft/

Microsoft Warns of New INC Ransomware Targeting U.S. Healthcare Sector
Source: https://thehackernews.com/2024/09/microsoft-warns-of-new-inc-ransomware.html

Data on Nearly 1 Million NHS Patients Leaked Online Following Ransomware Attack on London Hospitals
Source: https://therecord.media/data-on-nearly-1-million-nhs-patients-leaked-hospital-ransomware

Owner of Only US Platinum Mine Confirms Data Breach After Ransomware Claims
Source: https://therecord.media/stillwater-mining-company-montana-platinum-data-breach

Kransom Ransomware Disguised as a Game Through DLL Side-Loading
Source: https://hackread.com/ransomware-disguised-game-kransoms-attack-dll-side-loading/

Port of Seattle Refuses to Pay Rhysida Ransom Warns of Data Leak
Source: https://therecord.media/seattle-port-rhysida-ransom-refused

Sensitivity/ Handling Notice:
Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

ICS / SCADA / OT

Arkansas City Water Treatment Facility Switched to Manual Operations Following a Cyberattack
Source: https://securityaffairs.com/168871/hacking/arkansas-city-water-treatment-facility-cyberattack.html

Critical Flaws Found in VICIdial Contact Center Suite, PoC Published
Source: https://securityonline.info/critical-flaws-found-in-vicidial-contact-center-suite-cve-2024-8503-and-cve-2024-8504-poc-published/

CISA Urges Software Developers to Weed Out XSS Vulnerabilities
Source: https://www.bleepingcomputer.com/news/security/cisa-urges-software-devs-to-weed-out-xss-vulnerabilities/

Red Hat OpenShift Receives Patches for Two Critical Flaws
Source: https://securityonline.info/flaws-in-red-hat-openshift-cve-2024-45496-cve-2024-7387/

INDUSTRY UPDATES

Google Sees 68% Drop in Android Memory Safety Flaws Over 5 Years
Source: https://www.bleepingcomputer.com/news/security/google-sees-68-percent-drop-in-android-memory-safety-flaws-over-5-years/

Data Privacy Watchdog Files Complaint Against Mozilla for New Ad Tracking Feature
Source: https://therecord.media/noyb-europe-complaint-mozilla-firefox-privacy-preserving-attribution

Disney Ditching Slack After Massive July Data Breach
Source: https://www.bleepingcomputer.com/news/security/disney-ditching-slack-after-massive-july-data-breach/

Trends and Dangers in Open-Source Software Dependencies
Source: https://www.helpnetsecurity.com/2024/09/16/open-source-software-dependencies

FBI: Reported Cryptocurrency Losses Reached $5.6 Billion in 2023
Source: https://www.bleepingcomputer.com/news/security/fbi-reported-cryptocurrency-losses-reached-56-billion-in-2023/

The Bi-Weekly Cyber Rollup is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material. If you have any items that you would like to see added to the Bi-Weekly Cyber Rollup, you can contact the NDSLIC.

Email: ndslic@nd.gov NDSLIC: 701-328-8172

Sensitivity/ Handling Notice:

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.