Apr-03-23

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

April 3, 2023

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

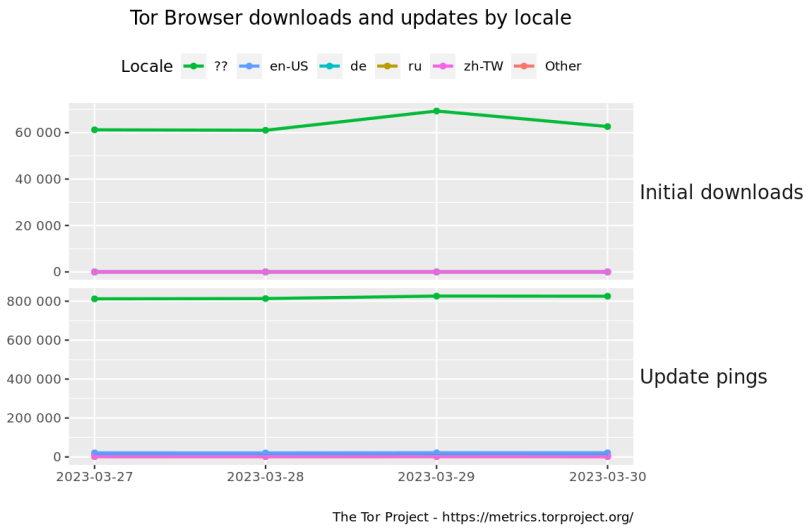
Internet Storm Center Infocon Status

The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

Index of Sections

Packet Storm Security

* Pinduoduo Is Straight Up Malware
* ChatGPT Banned In Italy Over Privacy Concerns
* Hacking Campaign Exploited Zero Day Tied To Spyware Firm
* Pro-Russia Cyber Gang Winter Vivern Puts US, Euro Lawmakers In Line Of Fire
* AlienFox Toolset Harvests Credentials From 18 Cloud Services
* Secret Trove Offers Rare Look Into Russian Cyberwar Ambitions
* Ironing Out The macOS Details Of A Smooth Operator
* Court Orders GitHub To Reveal Who Leaked Twitter's Source Code
* FDA Will Refuse New Medical Devices For Cybersecurity Reasons
* Pro-Russian Hackers Target Elected US Officials Supporting Ukraine
* Hackers Used Spyware Made In Spain To Target Users In The UAE
* BingBang: How A Simple Developer Mistake Could Have Led To Bing.com Takeover
* Meet APT43: The Group That Hacks, Spies, And Steals For North Korea's Ruling Elite
* AI Could Replace Equivalent Of 300 Million Jobs
* China Urges Apple To Improve Security And Privacy
* Ransomware Crooks Are Exploiting IBM File Exchange Bug
* New IcedID Malware Variants Shift From Banking Trojans To Ransomware
* Clearview AI Used Nearly 1m Times By US Police, It Tells The BBC
* North Dakota To Require Cybersecurity Education In Public Schools
* The FBI Has Been Buying Bulk Internet Data From Team Cymru
* US President Biden Kind Of Mostly Bans Commercial Spyware
* Twitter Takes Legal Action After Source Code Leaked Online
* Singapore Businesses Stumbling Over What Security Culture Entails
* Android App From China Executed Zero Day Exploit On Millions Of Devices
* Five Takeaways From TikTok CEO's Congress Grilling

Krebs on Security

* German Police Raid DDoS-Friendly Host 'FlyHosting'
* UK Sets Up Fake Booter Sites To Muddy DDoS Market
* Google Suspends Chinese E-Commerce App Pinduoduo Over Malware
* Why You Should Opt Out of Sharing Data With Your Mobile Provider
* Feds Charge NY Man as BreachForums Boss "Pompompurin"
* Microsoft Patch Tuesday, March 2023 Edition
* Two U.S. Men Charged in 2022 Hacking of DEA Portal
* Who's Behind the NetWire Remote Access Trojan?
* Sued by Meta, Freenom Halts Domain Registrations
* Highlights from the New U.S. Cybersecurity Strategy

Dark Reading

* 4 Steps for Shifting Left & Winning the Cybersecurity Battle
* Elastic Expands Cloud Security Capabilities for AWS
* The FDA's Medical Device Cybersecurity Overhaul Has Real Teeth, Experts Say
* Mimecast Report Reveals Nearly 60% of Companies in UAE and Saudi Arabia Need to Increase Cybersecurit
* Pro-Islam 'Anonymous Sudan' Hacktivists Likely a Front for Russia's Killnet Operation
* Adaptive Access Technologies Gaining Traction for Security, Agility
* Is Decentralized Identity About to Reach an Inflection Point?
* Vulkan Playbook Leak Exposes Russia's Plans for Worldwide Cyberwar
* US Space Force Requests $700M for Cybersecurity Blast Off
* What CISOs Can Do to Build Trust & Fight Fraud in the Metaverse
* Post-Quantum Satellite Protection Rockets Towards Reality
* Automatic Updates Deliver Malicious 3CX 'Upgrades' to Enterprises
* BEC Fraudsters Expand to Snatch Real-World Goods in Commodities Twist
* How to Solve IoT's Identity Problem
* Microsoft Patches 'Dangerous' RCE Flaw in Azure Cloud Service
* Organizations Consider Self-Insurance to Manage Risk
* DataDome Closes $42M in Series C Funding to Advance the Fight Against Bot-Driven Cyberattacks and Fra
* Socura Launches Managed SASE (MSASE) Service
* Stop Blaming the End User for Security Risk
* Spera Takes Aim at Identity Security Posture Management

The Hacker News

* Western Digital Hit by Network Security Breach - Critical Services Disrupted!
* Italian Watchdog Bans OpenAI's ChatGPT Over Data Protection Concerns
* "It's The Service Accounts, Stupid": Why Do PAM Deployments Take (almost) Forever To Complete
* Crypto-Stealing OpcJacker Malware Targets Users with Fake VPN Service
* Microsoft Fixes New Azure AD Vulnerability Impacting Bing Search and Major Apps
* Cacti, Realtek, and IBM Aspera Faspex Vulnerabilities Under Active Exploitation
* Hackers Exploiting WordPress Elementor Pro Vulnerability: Millions of Sites at Risk!
* Winter Vivern APT Targets European Government Entities with Zimbra Vulnerability
* Cyber Police of Ukraine Busted Phishing Gang Responsible for $4.33 Million Scam
* Deep Dive Into 6 Key Steps to Accelerate Your Incident Response
* 3CX Supply Chain Attack - Here's What We Know So Far
* Researchers Detail Severe "Super FabriXss" Vulnerability in Microsoft Azure SFX
* Chinese RedGolf Group Targeting Windows and Linux Systems with KEYPLUG Backdoor
* New Wi-Fi Protocol Security Flaw Affecting Linux, Android and iOS Devices
* Cyberstorage: Leveraging the Multi-Cloud to Combat Data Exfiltration

Security Week

* Microsoft OneNote Starts Blocking Dangerous File Extensions
* US Defense Department Launches 'Hack the Pentagon' Website
* Western Digital Shuts Down Services Due to Cybersecurity Breach
* 4.8 Million Impacted by Data Breach at TMX Finance
* Europe, North America Most Impacted by 3CX Supply Chain Hack
* TikTok Attorney: China Can't Get U.S. Data Under Plan
* Italy Temporarily Blocks ChatGPT Over Privacy Concerns
* FDA Announces New Cybersecurity Requirements for Medical Devices
* Report: Chinese State-Sponsored Hacking Group Highly Active
* Votiro Raises $11.5 Million to Prevent File-Borne Threats

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [Live Demo] Ridiculously Easy Security Awareness Training and Phishing
* Mid-Sized Businesses Lack the Staffing, Expertise, and Resources to Defend Against Cyberattacks
* Majority of Government Employees are Partially Working Virtually Despite Increased User-Related Cyber
* Fake ChatGPT Scam Turns into a Fraudulent Money-Making Scheme
* The New Face of Fraud: FTC Sheds Light on AI-Enhanced Family Emergency Scams
* Artificial Intelligence Makes Phishing Text More Plausible
* The Pope, Puff Jackets and Money going POOF!
* Australian Police Arrest Business Email Compromise (BEC) Operators
* [LIVE DEMO] Are Your Users Making Risky Security Mistakes? Deliver Real-Time Coaching in Respons
* The FBI's Public Service Warning of Business Email Compromise

ISC2.org Blog

* New adaptive platform customizes online certification training for a personalized experience
* CISA Moving Further Towards Pre-Emptive Stance with Ransomware Attack Alert System
* Latest Cyberthreats and Advisories - March 31, 2023
* New CISSP Exam Registration Process for 2023
* Analysis: Hackers Exploit Zero-Day to Siphon $1.5 Million From Bitcoin ATMs

HackRead

* Mullvad VPN and Tor Project Release Mullvad Browser
* Ukrainian Hacktivists Trick Russian Military Wives for Personal Info
* Zimbra email platform vulnerability exploited to steal European govt emails
* Italy Temporarily Blocks ChatGPT, Citing Privacy Issues
* New Cylance Ransomware Targets Linux and Windows, Warn Researchers
* Ukraine Busts Gang for Massive $4.3 Million Phishing Scams
* CISA Warns of Vulnerabilities in Propump and Controls' Osprey Pump Controller

Koddos

* Mullvad VPN and Tor Project Release Mullvad Browser
* Ukrainian Hacktivists Trick Russian Military Wives for Personal Info
* Zimbra email platform vulnerability exploited to steal European govt emails
* Italy Temporarily Blocks ChatGPT, Citing Privacy Issues
* New Cylance Ransomware Targets Linux and Windows, Warn Researchers
* Ukraine Busts Gang for Massive $4.3 Million Phishing Scams
* CISA Warns of Vulnerabilities in Propump and Controls' Osprey Pump Controller

Naked Security

* World Backup Day is here again - 5 tips to keep your precious data safe
* Supply chain blunder puts 3CX telephone app users at risk
* S3 Ep128: So you want to be a cybercriminal? [Audio + Text]
* Cops use fake DDoS services to take aim at wannabe cybercriminals
* Apple patches everything, including a zero-day fix for iOS 15 users
* Microsoft assigns CVE to Snipping Tool bug, pushes patch to Store
* In Memoriam - Gordon Moore, who put the more in "Moore's Law"
* WooCommerce Payments plugin for WordPress has an admin-level hole - patch now!
* S3 Ep127: When you chop someone out of a photo, but there they are anyway…
* Windows 11 also vulnerable to "aCropalypse" image data leakage

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

IBM Security Intelligence

* Is It Time to Start Hiding Your Work Emails?
* 2022 Industry Threat Recap: Finance and Insurance
* And Stay Out! Blocking Backdoor Break-Ins
* X-Force Prevents Zero Day from Going Anywhere
* Cyber Storm Predicted at the 2023 World Economic Forum
* Remote Employees: Update Your Routers (and More WFH IT Tips)
* The Role of Human Resources in Cybersecurity
* New Attack Targets Online Customer Service Channels
* Cybersecurity 101: What is Attack Surface Management?
* Six Ways to Secure Your Organization on a Smaller Budget

InfoWorld

* If you want a career in AI, learn Python
* 5 priorities that cut cloud costs and improve IT ops
* Climate change: The push to reduce IT's carbon footprint
* Visual Studio Code 1.77 previews GitHub Copilot chat
* The 'AI tax' on AI-enabled applications in the cloud
* How ChatGPT will enable the 100x programmer
* What is Apache Spark? The big data platform that crushed Hadoop
* MariaDB SkySQL adds serverless analytics, cost management features
* JetBrains updates IDEs for Java, JavaScript, Ruby
* How to use the rate limiting middleware in ASP.NET Core 7

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

The Hacker Corner

Conferences

* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems
* Exploiting null-dereferences in the Linux kernel

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* DamCTF 2023
* Bucket CTF 2023
* cursedCTF 2023
* Midnight Sun CTF 2023 Quals
* YetiCTF2023
* HackPack CTF 2023
* Midnight Flag - Black Box
* PlaidCTF 2023
* JerseyCTF III
* Summit CTF

VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

Tools & Techniques

Packet Storm Security Tools Links

* Global Socket 1.4.40
* GRR 3.4.6.7
* OpenSSL Toolkit 3.1.0
* OpenSSH 9.3p1
* I2P 2.2.0
* Packet Fence 12.2.0
* AIDE 0.18.1
* Wireshark Analyzer 4.0.4
* Zeek 5.0.7
* AIEngine 2.3.0

Kali Linux Tutorials

* Hunxploit04 - A new OSINT Tools for Information Gathering
* FindUncommonShares A Python Equivalent Of PowerView's Invoke-ShareFinder.ps1 Allowing To Quickly Fin
* GPT_Vuln-analyzer : Uses ChatGPT API And Python-Nmap Module To Use The GPT3 Model To Create Vulnerabi
* CertVerify : A Scanner That Files With Compromised Or Untrusted Code Signing Certificates
* CertWatcher : A Tool For Capture And Tracking Certificate Transparency Logs, Using YAML Templates Bas
* MacOSThreatTrack : Bash Tool Used For Proactive Detection Of Malicious Activity On macOS Systems
* Graphicator : A GraphQL Enumeration And Extraction Tool
* DataSurgeon : Quickly Extracts IP's, Email Addresses, Hashes, Files, Credit Cards, Social Secuirty Nu
* Thunderstorm : Modular Framework To Exploit UPS Devices
* RedTeam-Physical-Tools : Red Team Toolkit Used In The Field For Physical Security, Red Teaming, And T

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Memory Forensics: How we used to do it & how we use it to respond to large-scale breaches today
* 意外と簡単なランサムウェア運用ツールの検出と駆逐
* Detecting & Hunting Ransomware Operator Tools: It Is Easier Than You Think!
* Why should you take the FOR308: Digital Forensics Essentials?

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

* Cerebral App Leaks Telehealth Medical Data - ThreatWire
* NEW Powershell features in DuckyScript 3.0
* UEFI Bootkit Successfully Hits Windows 11 - ThreatWire

The PC Security Channel [TPSC]

* The Malware that hacked Linus Tech Tips
* Ransomware Decryption: Free Tools

Eli the Computer Guy

* 9,000 MORE LAYOFFS at AMAZON - eBeggar Wednesday
* CHATGPT INTRO - Silicon Dojo Seminar
* 10,000 MORE LAYOFFS at FACEBOOK/ META - eBeggar Wednesday
* DJANGO INTRO - Seminar for Silicon Dojo

Security Now

* Microsoft's Email Extortion - Pwn2Own, Edge Crypto Wallet
* Flying Trojan Horses - Exynos 0-days, TikTok Tick Tock, 90-day TLS cert life, CHESS is safe!

Troy Hunt

* Weekly Update 341

Intel Techniques: The Privacy, Security, & OSINT Show

* 292-Vital News & Updates
* 291-Mobile App Security & Audio Transcription

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Judging Management System 1.0 Shell Upload
* Judging Management System 1.0 SQL Injection
* EQ Enterprise Management System 2.2.0 SQL Injection
* Online Pizza Ordering 1.0 SQL Injection
* rconfig 3.9.7 SQL Injection
* CoolerMaster MasterPlus 1.8.5 Unquoted Service Path
* Qubes Mirage Firewall 0.8.3 Denial Of Service
* WordPress WooCommerce 7.1.0 Remote Code Execution
* Cacti 1.2.22 Remote Command Execution
* Textpattern 4.8.8 Remote Code Execution
* Bludit 3-14-1 Shell Upload
* Ancillary Function Driver (AFD) For Winsock Privilege Escalation
* Eve-ng 5.0.1-13 Cross Site Scripting
* WordPress WPForms 1.7.8 Cross Site Scripting
* Forcepoint (Stonesoft VPN Client) 6.2.0 / 6.8.0 Local Privilege Escalation
* CrowdStrike Falcon Agent 6.44.15806 Uninstall Issue
* Lavasoft 4.1.0.409 Unquoted Service Path
* Virtual Reception 1.0 Directory Traversal
* Covenant 0.5 Remote Code Execution
* DSL-124 Wireless N300 ADSL2+ Backup Disclosure
* myBB forums 1.8.26 Cross Site Scripting
* Dreamer CMS 4.0.0 SQL Injection
* Helmet Store Showroom 1.0 SQL Injection
* Uniview NVR301-04S2-P4 Cross Site Scripting
* Inbit Messenger 4.9.0 Remote Command Execution

CXSecurity

* Scdbg 1.0 Buffer overflow DoS
* Sysax Multi Server 6.95 Password Denial of Service (PoC)
* Scdbg 1.0 Denial Of Service
* Linksys AX3200 V1.1.00 Command Injection
* Microsoft User Account Control Nuances
* Apache Tomcat Privilege Escalation
* Webpower UPS 5.53 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

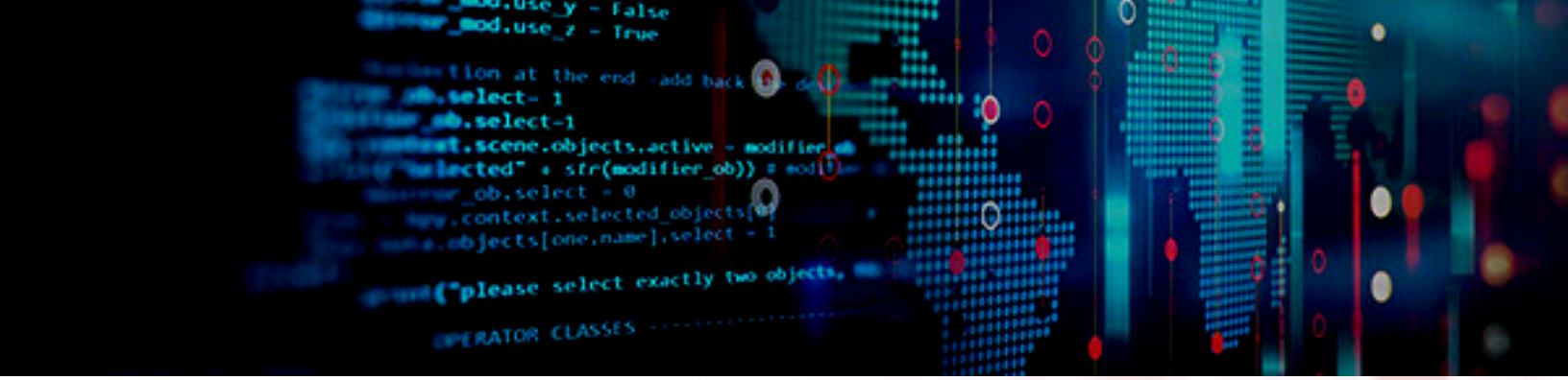
* [webapps] Active eCommerce CMS 6.5.0 - Stored Cross-Site Scripting (XSS)
* [webapps] ERPGo SaaS 3.9 - CSV Injection
* [webapps] AmazCart CMS 3.4 - Cross-Site-Scripting (XSS)
* [webapps] SQL Monitor 12.1.31.893 - Cross-Site Scripting (XSS)
* [local] sudo 1.8.0 to 1.9.12p1 - Privilege Escalation
* [webapps] Art Gallery Management System Project v1.0 - SQL Injection (sqli) authenticated
* [webapps] Art Gallery Management System Project v1.0 - SQL Injection (sqli) Unauthenticated
* [webapps] Art Gallery Management System Project v1.0 - Reflected Cross-Site Scripting (XSS)
* [webapps] MyBB 1.8.32 - Remote Code Execution (RCE) (Authenticated)
* [local] Microsoft Exchange Active Directory Topology 15.02.1118.007 - 'Service MSExchangeADTopology'
* [webapps] SLIMSV 9.5.2 - Cross-Site Scripting (XSS)
* [local] Chromacam 4.0.3.0 - PsyFrameGrabberService Unquoted Service Path
* [local] Solaris 10 libXm - Buffer overflow Local privilege escalation
* [webapps] Zstore 6.5.4 - Reflected Cross-Site Scripting (XSS)
* [local] HotKey Clipboard 2.1.0.6 - Privilege Escalation Unquoted Service Path
* [webapps] Nacos 2.0.3 - Access Control vulnerability
* [webapps] Metform Elementor Contact Form Builder v3.1.2 - Unauthenticated Stored Cross-Site Scripting
* [local] Windows 11 10.0.22000 - Backup service Privilege Escalation
* [webapps] ChiKoi v1.0 - SQL Injection
* [webapps] pimCore v5.4.18-skeleton - Sensitive Cookie with Improper SameSite Attribute
* [webapps] ELSI Smart Floor V3.3.3 - Stored Cross-Site Scripting (XSS)
* [local] NetIQ/Microfocus Performance Endpoint v5.1 - remote root/SYSTEM exploit
* [webapps] Yahoo User Interface library (YUI2) TreeView v2.8.2 - Multiple Reflected Cross Site Scripti
* [dos] AimOne Video Converter V2.04 Build 103 - Buffer Overflow (DoS)
* [remote] Nexxt Router Firmware 42.103.1.5095 - Remote Code Execution (RCE) (Authenticated)

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

user@yourlinux:~$ *searchsploit keyword1 keyword2*

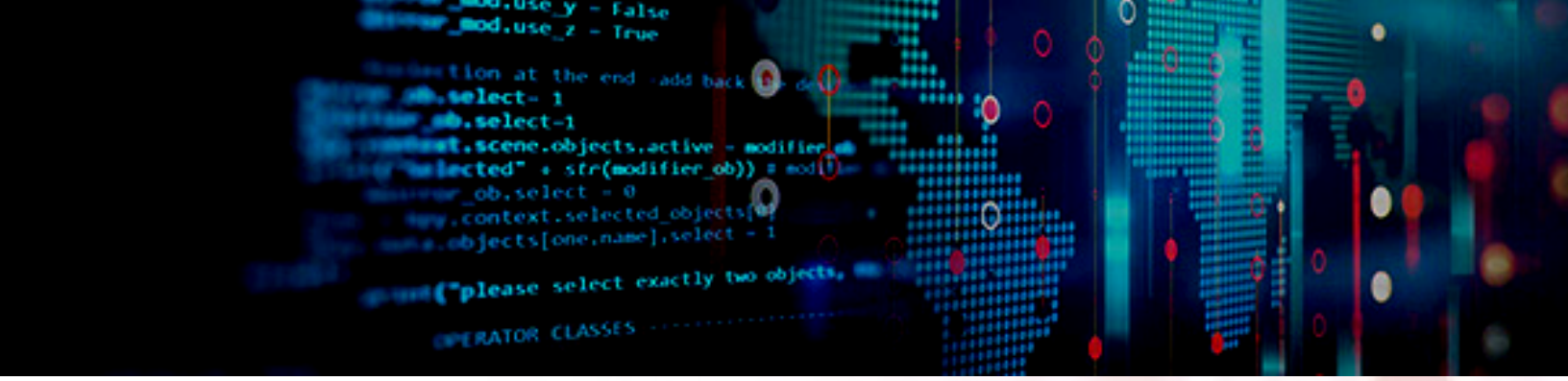
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://spw.crecisp.gov.br/xx.txt
https://spw.crecisp.gov.br/xx.txt notified by xstro0
https://www.crecisp.gov.br/xx.txt
https://www.crecisp.gov.br/xx.txt notified by xstro0
https://cemapi.gouv.ml/kurd.html
https://cemapi.gouv.ml/kurd.html notified by 0x1998
https://www.nongnamsaisao.go.th/kurd.html
https://www.nongnamsaisao.go.th/kurd.html notified by 0x1998
https://mukomukokab.go.id/zz.html
https://mukomukokab.go.id/zz.html notified by xNot_RespondinGx
https://bpbd.mukomukokab.go.id/lol.txt
https://bpbd.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
https://chapadagaucha.mg.gov.br/nda.txt
https://chapadagaucha.mg.gov.br/nda.txt notified by NDA
https://dinkes.pareparekota.go.id/-.php
https://dinkes.pareparekota.go.id/-.php notified by Newbie_Tersakiti
http://pengadilan-dev.subang.go.id/ar.php
http://pengadilan-dev.subang.go.id/ar.php notified by Indonesia Attacker
https://cipunagara.dev.subang.go.id/ar.php
https://cipunagara.dev.subang.go.id/ar.php notified by Indonesia Attacker
https://polres.dev.subang.go.id/ar.php
https://polres.dev.subang.go.id/ar.php notified by Indonesia Attacker
https://rsud.dev.subang.go.id/ar.php
https://rsud.dev.subang.go.id/ar.php notified by Indonesia Attacker
http://web.seducoahuila.gob.mx/consejo/fotos/05DST0003A_5_org0n.pdf
http://web.seducoahuila.gob.mx/consejo/fotos/05DST0003A_5_org0n.pdf notified by org0n
http://www.huanucoagrario.gob.pe/documento/org0n.pdf
http://www.huanucoagrario.gob.pe/documento/org0n.pdf notified by org0n
https://fomentoempresarial.tlajomulco.gob.mx/system/
https://fomentoempresarial.tlajomulco.gob.mx/system/ notified by org0n
https://citasenlinea.tlajomulco.gob.mx/system/
https://citasenlinea.tlajomulco.gob.mx/system/ notified by org0n
http://oomsapaloreto.gob.mx/1/subir/archivos/org0n.pdf
http://oomsapaloreto.gob.mx/1/subir/archivos/org0n.pdf notified by org0n

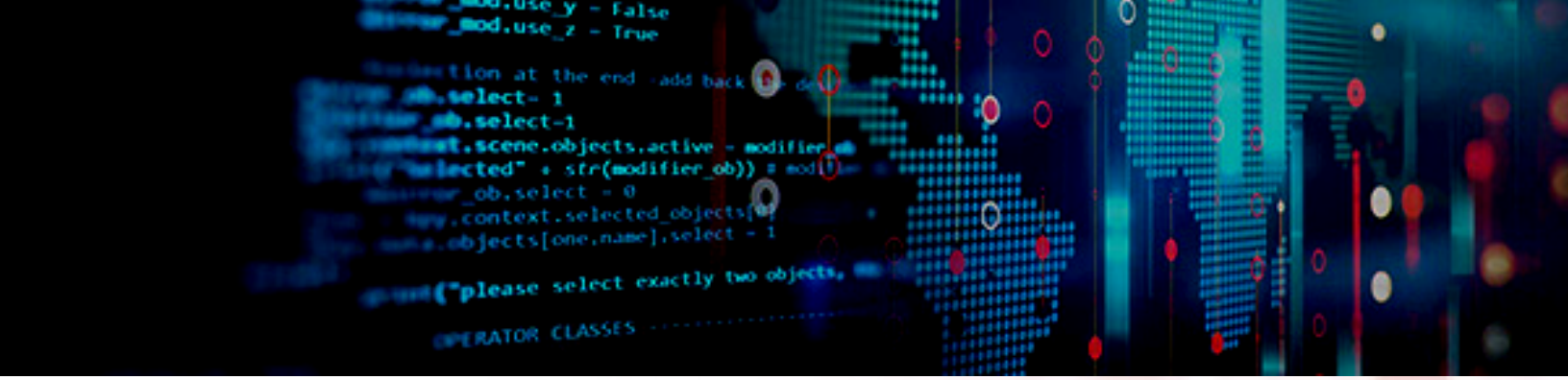


Dark Web News

Darknet Live

[Polish Man Sentenced for Distributing Drugs on the Dark Web]
[Illicit Weapons and Cannabis Reseller Imprisoned]
[Three Men Imprisoned for Distributing Counterfeit Oxycodone Pills]
[Two Years in Prison Against a Dark Web Drugs Vendor]

Dark Web Link



Trend Micro Anti-Malware Blog

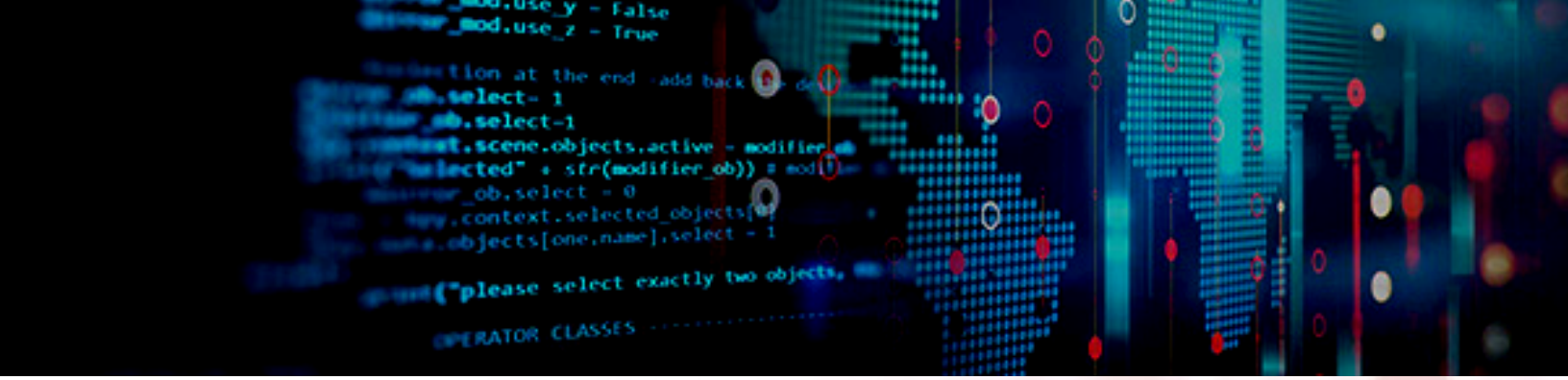
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-up
* What's New in InsightVM and Nexpose: Q1 2023 in Review
* Velociraptor Version 0.6.8 Available Now
* Rapid7 Announces Partner of the Year Awards 2023 Winners
* Backdoored 3CXDesktopApp Installer Used in Active Threat Campaign
* Executive Webinar: Confronting Security Fears to Control Cyber Risk, Part Three
* Multiple Vulnerabilities in Rocket Software UniRPC server (Fixed)
* What's New in InsightIDR: Q1 2023 in Review
* Active Exploitation of IBM Aspera Faspex CVE-2022-47986
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* Mozilla Releases Security Update for Thunderbird 102.9.1
* Samba Releases Security Updates for Multiple Versions of Samba
* CISA Adds Ten Known Exploited Vulnerabilities to Catalog
* CISA Releases One Industrial Control Systems Advisory
* Supply Chain Attack Against 3CXDesktopApp
* Apple Releases Security Updates for Multiple Products
* Untitled Goose Tool Aids Hunt and Incident Response in Azure, Azure Active Directory, and Microsoft 3
* JCDC Cultivates Pre-Ransomware Notification Capability
* #StopRansomware: LockBit 3.0
* Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server
* Vulnerability Summary for the Week of April 30, 2007
* Vulnerability Summary for the Week of October 22, 2012

Zero Day Initiative Advisories

ZDI-CAN-20669: Oracle
A CVSS score 6.0 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Bien Pham (@bienpnn) from Qrious Security (@qriousec)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20743: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20746: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20744: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20747: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until

2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20719: VMware

A CVSS score 6.0 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Nguy\xe1\xbb\x85n Ho\xc3\xa0ng Th\xe1\xba\xa1ch (@hi_im_d4rkn3ss) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20773: VMware

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Nguy\xe1\xbb\x85n Ho\xc3\xa0ng Th\xe1\xba\xa1ch (@hi_im_d4rkn3ss) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20712: Adobe

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20733: Tesla

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'David BERARD (@_p0ly_) and Vincent DEHORS (@vdehors) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20722: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20749: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nguy\xe1\xbb\x85n Ti\xe1\xba\xbfn Giang (@testanull) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20671: Oracle

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'dungdm(@_piers2) of Viettel Cyber Security' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20734: Tesla

A CVSS score 9.0 (AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'David BERARD (@_p0ly_) and Vincent DEHORS (@vdehors) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20670: Oracle

A CVSS score 6.0 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'dungdm(@_piers2) of Viettel Cyber Security' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a

patch we will coordinate the release of a public advisory.

ZDI-CAN-20723: Oracle

A CVSS score 6.0 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Thomas BOUZERAR (@MajorTomSec) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20716: Microsoft

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nguy\xe1\xbb\x85n Ti\xe1\xba\xbfn Giang (@testanull) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20737: Tesla

A CVSS score 4.6 (AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'David BERARD (@_p0ly_) and Vincent DEHORS (@vdehors) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20748: Microsoft

A CVSS score 4.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Nguy\xe1\xbb\x85n Ti\xe1\xba\xbfn Giang (@testanull) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20779: Oracle

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Bien Pham (@bienpnn) from Qrious Security (@qriousec)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20736: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Thomas Imbert (@masthoon) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20714: Apple

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Eloi Benoist-Vanderbeken (@elvanderb) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-03-30, 4 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20630: Ashlar-Vellum

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-03-22, 12 days ago. The vendor is given until 2023-07-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20229: Samba

A CVSS score 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Florent Saudel (@thalium_team)' was reported to the affected vendor on: 2023-03-22, 12 days ago. The vendor is given until 2023-07-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20660: Ashlar-Vellum

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-03-22, 12 days ago. The vendor is given until 2023-07-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5990-1

Ubuntu Security Notice 5990-1 - It was discovered that musl did not handle certain i386 math functions properly. An attacker could use this vulnerability to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. It was discovered that musl did not handle wide-character conversion properly. A remote attacker could use this vulnerability to cause resource consumption , denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS.

Ubuntu Security Notice USN-5989-1

Ubuntu Security Notice 5989-1 - Tao Lyu discovered that GlusterFS did not properly handle certain event notifications. An attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5988-1

Ubuntu Security Notice 5988-1 - It was discovered that integer overflows vulnerabilities existed in Xcftools. An attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5986-1

Ubuntu Security Notice 5986-1 - Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Debian Security Advisory 5380-1

Debian Linux Security Advisory 5380-1 - Jan-Niklas Sohn discovered that a user-after-free flaw in the Composite extension of the X.org X server may result in privilege escalation if the X server is running under the root user.

Red Hat Security Advisory 2023-1514-01

Red Hat Security Advisory 2023-1514-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.10 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.9, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.10 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, denial of service, deserialization, and information leakage vulnerabilities.

Kernel Live Patch Security Notice LNS-0093-1

Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. It was discovered that the Upper Level Protocol (ULP) subsystem in the Linux kernel did not properly handle sockets entering the LISTEN state in certain protocols, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

Red Hat Security Advisory 2023-1513-01

Red Hat Security Advisory 2023-1513-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.10 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.9, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.10 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, denial of service, deserialization, and information leakage vulnerabilities.

Ubuntu Security Notice USN-5985-1

Ubuntu Security Notice 5985-1 - It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service. It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle

indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs.

Red Hat Security Advisory 2023-1310-01

Red Hat Security Advisory 2023-1310-01 - An update is now available for Logging Subsystem for Red Hat OpenShift - 5.5.9. Red Hat Product Security has rated this update as having a security impact of Moderate.

Red Hat Security Advisory 2023-1512-01

Red Hat Security Advisory 2023-1512-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.10 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.9 and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.10 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, denial of service, deserialization, and information leakage vulnerabilities.

Ubuntu Security Notice USN-5987-1

Ubuntu Security Notice 5987-1 - It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-1529-01

Red Hat Security Advisory 2023-1529-01 - Service Telemetry Framework provides automated collection of measurements and data from remote clients, such as Red Hat OpenStack Platform or third-party nodes. STF then transmits the information to a centralized, receiving Red Hat OpenShift Container Platform deployment for storage, retrieval, and monitoring. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5983-1

Ubuntu Security Notice 5983-1 - Cyku Hong discovered that Nette was not properly handling and validating data used for code generation. A remote attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5984-1

Ubuntu Security Notice 5984-1 - It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service. It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-1392-01

Red Hat Security Advisory 2023-1392-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.10.55.

Red Hat Security Advisory 2023-1393-01

Red Hat Security Advisory 2023-1393-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.55.

Ubuntu Security Notice USN-5981-1

Ubuntu Security Notice 5981-1 - It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service. It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5982-1

Ubuntu Security Notice 5982-1 - It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. It was discovered that a

use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5980-1

Ubuntu Security Notice 5980-1 - It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service. It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs.

Ubuntu Security Notice USN-5686-4

Ubuntu Security Notice 5686-4 - USN-5686-1 fixed several vulnerabilities in Git. This update provides the corresponding fix for CVE-2022-39253 on Ubuntu 16.04 ESM. Cory Snider discovered that Git incorrectly handled certain symbolic links. An attacker could possibly use this issue to cause an unexpected behaviour.

Ubuntu Security Notice USN-5979-1

Ubuntu Security Notice 5979-1 - It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. It was discovered that a race condition existed in the Xen network backend driver in the Linux kernel when handling dropped packets in certain circumstances. An attacker could use this to cause a denial of service.

Debian Security Advisory 5379-1

Debian Linux Security Advisory 5379-1 - Kim Alvefur discovered that insufficient message sender validation in dino-im, a modern XMPP/Jabber client, may result in manipulation of entries in the personal bookmark store without user interaction via a specially crafted message. Additionally an attacker can take advantage of this flaw to change how group chats are displayed or force a user to join or leave an attacker-selected groupchat.

Ubuntu Security Notice USN-5978-1

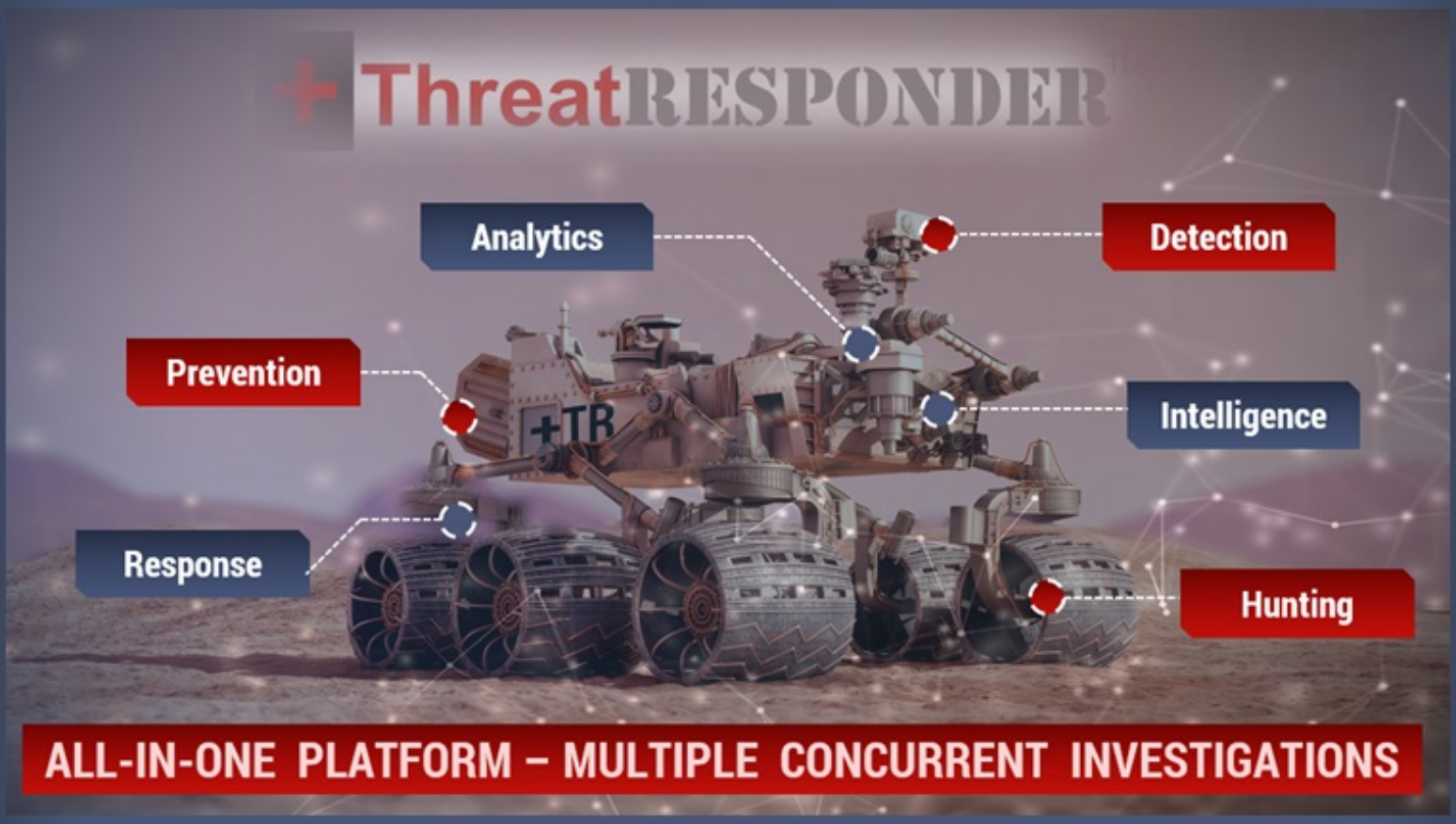
Ubuntu Security Notice 5978-1 - It was discovered that the network queuing discipline implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



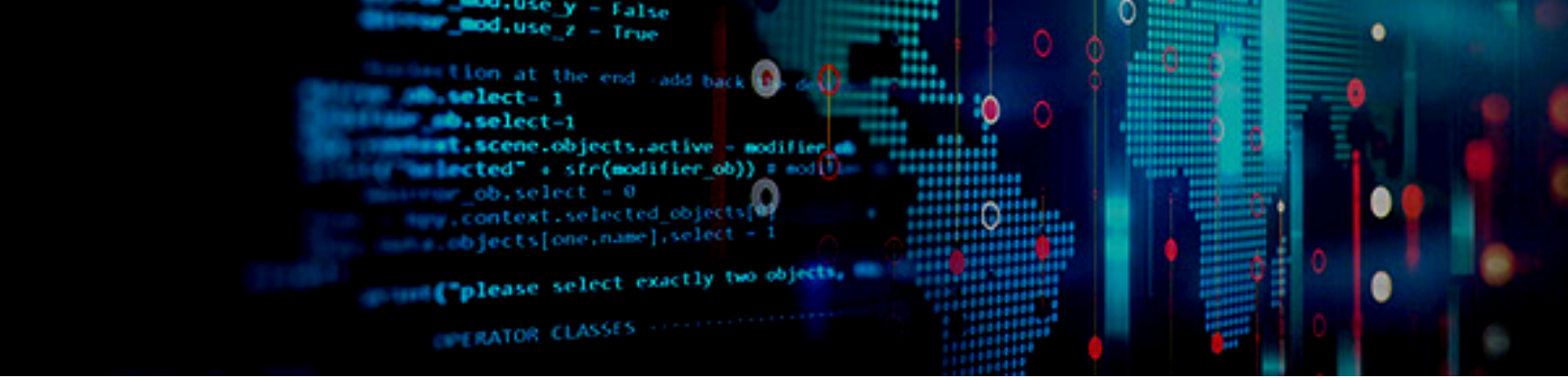
The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

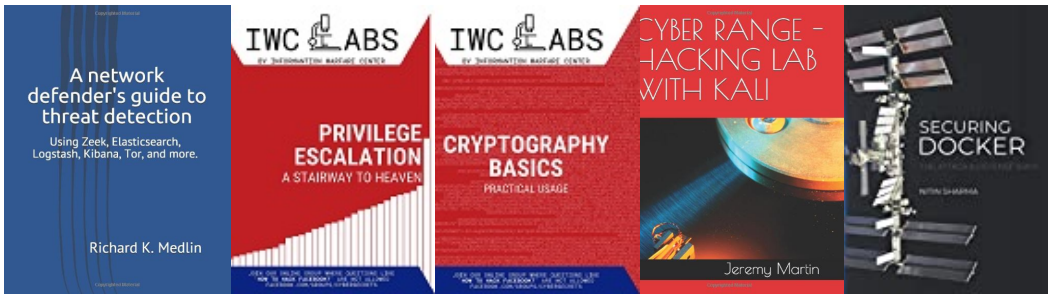


The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP