CYBER WAR

WEEKLY AWARENESS REPORT

04-20-20

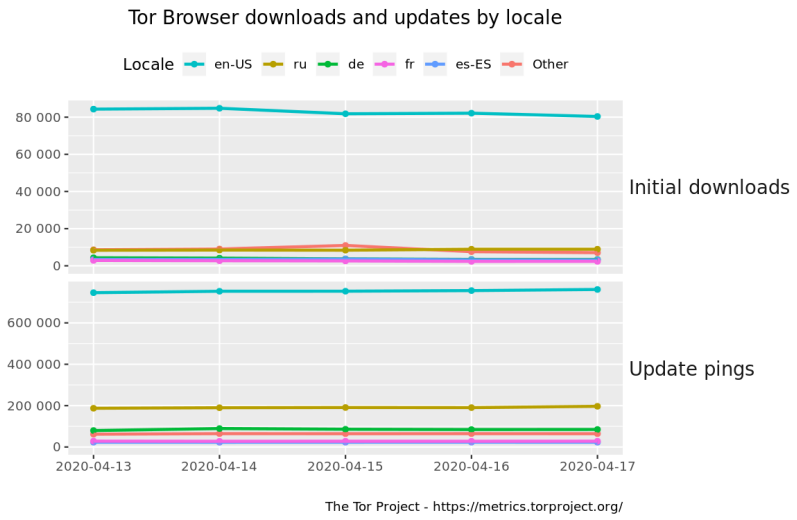
April 20, 2020

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

Symantec ThreatCon Low: Basic network posture

This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms should be used.



Interesting News

* CTF: Avengers Arsenal Challenge

The Challenge… Using whatever tool of your choice. Capture all the flags you can, identify and exploit as many vulnerabilities as you can, write a report, and write a walk through on how you found each item within. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents... Sign up for the CTF Now!for more details.

* * We have an active Facebook group that discusses topics ranging from computer forensics to ethical hacking and more. Join the Cyber Secrets Facebook group here. If you would like to receive the CIR updates by email, Subscribe!

Index of Sections

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* Naked Security
* Quick Heal - Security Simplified
* Threat Post

The Hacker Corner:
* Security Conferences
* Zone-H Latest Published Website Defacements

Tools & Techniques
* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis
* CSI Linux

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Advisories
* US-Cert (Current Activity-Alerts-Bulletins)
* Symantec's Latest List
* Packet Storm Security's Latest List

Credits

Packet Storm Security

* Judge Rules Against Twitter Transparency Effort
* Hackers Steal $25 Million Worth Of Cryptocurrency From Uniswap And Lendf.me
* Hacker Leaks 23 Million Accounts From Webkinz Children's Game
* Tor Project Loses A Third Of Staff In Coronavirus Cuts
* PoetRAT Trojan Targets Energy Sector Using Coronavirus Lures
* Cisco IP Phone Harbors Critical RCE Flaw
* Google Blocked 126 Million COVID-19 Phishing Scams In One Week
* Poorly Secured Docker Image Comes Under Rapid Attack
* US-CERT Reiterates $5 Million Bounty On North Korean Hackers
* Kernel Vulns In Android Devices Using Qualcomm Chips Explored
* Coronavirus: Facebook Alerts Users Exposed To Misinformation
* Hackers Are Selling A Critical Zoom Zero-Day Exploit For $500,000
* Intel Fixes High-Severity Flaws In NUC, Discontinues Buggy Compute Module
* Apple Tracks Changes In Pandemic Travel Behavior
* Google Axes 49 Malicious Chrome Extensions From Web Store
* Hospitals Must Secure Vital Backend Networks Before It's Too Late
* Russian State Hackers Behind San Francisco Airport Hack
* Account Details For 4 Million Quidd Users Shared On Hacking Forum
* TikTok Flaw Allows Hackers To Plant Forged Videos
* Zoom: Every Security Issue Uncovered In The Video Chat App
* Facebook Must Face Renewed Privacy Lawsuit Over User Tracking
* Citing BGP Hijacks And Hack Attacks, Feds Want China Telecom Out Of The US
* Ransomware Scumbags Release Confidential Docs
* SEC Settles With Two Suspects In EDGAR Hacking Case
* Officials Say State-Backed Hackers Taking Advantage Of Outbreak

Krebs on Security

* Sipping from the Coronavirus Domain Firehose
* COVID-19 Has United Cybersecurity Experts, But Will That Unity Survive the Pandemic?
* Microsoft Patch Tuesday, April 2020 Edition
* New IRS Site Could Make it Easy for Thieves to Intercept Some Stimulus Payments
* Microsoft Buys Corp.com So Bad Guys Can't
* 'War Dialing' Tool Exposes Zoom's Password Problems
* Phish of GoDaddy Employee Jeopardized Escrow.com, Among Others
* Annual Protest to 'Fight Krebs' Raises â,¬150K+
* Russians Shut Down Huge Card Fraud Ring
* US Government Sites Give Bad Security Advice

Dark Reading

* COVID-19 Caption Contest Winners
* Remote Access Makes a Comeback: 4 Security Challenges in the Wake of COVID-19
* COVID-19: Latest Security News & Commentary
* Pen-Test Results Hint at Improvements in Enterprise Security
* COVID-Themed Phishing Messages Fill Phishing Filters on Gmail
* Researchers Explore Details of Critical VMware Vulnerability
* Cybersecurity Home-School: The Robot Project
* 'Look for the Helpers' to Securely Enable the Remote Workforce
* 10 Standout Security M&A Deals from Q1 2020
* Could Return of Ghost Squad Hackers Signal Rise in COVID-19-Related Hactivism?
* Neglected Infrastructure, Invasive Tech to Plague Infosec in 2022
* Massive Bot-Enabled Ad Fraud Campaign Targeted Connected TVs
* Small Business Is Big Target for Ransomware
* 4 Cybersecurity Lessons from the Pandemic
* Post Pandemic, Technologists Pose Secure Certification for Immunity
* Arxan Technologies Joins New Software Company Digital.ai
* 5 Things Ransomware Taught Me About Responding in a Crisis
* How Enterprises Are Developing and Maintaining Secure Applications
* New Malware Family Assembles IoT Botnet
* DHS Issues Alert for New North Korean Cybercrime

The Hacker News

* COVID-Themed Lures Target SCADA Sectors With Data Stealing Malware
* CISA Warns Patched Pulse Secure VPNs Could Still Expose Organizations to Hackers
* Why SaaS opens the door to so many cyber threats (and how to make it safer)
* Over 700 Malicious Typosquatted Libraries Found On RubyGems Repository
* How to transform your revolutionary idea into a reality: $100K Nokia Bell Labs Prize
* U.S. Offers Rewards up to $5 Million for Information on North Korean Hackers
* 49 New Google Chrome Extensions Caught Hijacking Cryptocurrency Wallets
* Microsoft Issues Patches for 3 Bugs Exploited as Zero-Day in the Wild
* Dell Releases A New Cybersecurity Utility To Detect BIOS Attacks
* Hackers Targeting Critical Healthcare Facilities With Ransomware During Coronavirus Pandemic
* Webinar: How MSSPs Can Overcome Coronavirus Quarantine Challenges
* Google and Apple Plan to Turn Phones into COVID-19 Contact-Tracking Devices
* 7 Ways Hackers and Scammers Are Exploiting Coronavirus Panic
* Dark Nexus: A New Emerging IoT Botnet Malware Spotted in the Wild
* Unveiled: How xHelper Android Malware Re-Installs Even After Factory Reset

Security Week

* Coronavirus Crisis Forces Tor Project Layoffs
* Patching Pulse Secure VPN Not Enough to Keep Attackers Out, CISA Warns
* Pompeo Concerned by Cyber Attacks on Czech Hospitals
* Massachusetts, Indiana Settle With Equifax Over 2017 Data Breach
* LED Light Control Console Abused to Spew Malware
* Twitter Fails to Obtain Permission to Disclose Surveillance Requests
* Maze Ransomware Caused Disruptions at Cognizant
* Hackers Targeting Azerbaijan Show Interest in SCADA Systems
* Several Botnets Using Zero-Day Vulnerability to Target Fiber Routers
* Google Sees Millions of COVID-19-Related Malicious Emails Daily
* Ad Fraud Operation Accounted for Large Amount of Connected TV Traffic
* DHS Working on Cloud-based Root-of-Trust to Secure Agency Email on Mobile Devices
* GitHub Shares Details on Six Chrome Vulnerabilities
* GitHub Warns Users of Sophisticated Phishing Campaign
* Financial Phishing Jumped to 51% of All Phishing in 2019: Kaspersky
* Cisco Patches Critical Flaws in IP Phones, UCS Director
* Zoom Rolls Out New Measures as Security Fears Mount
* Details Released for Flaw Allowing Full Control Over VMware Deployments
* 'Not a Safe Platform': India Bans Zoom for Government Use
* Double Extortion: Ransomware's New Normal Combining Encryption with Data Theft

Infosecurity Magazine

* US Bans Church Website Selling #COVID19 'Miracle' Treatment
* HMRC #COVID19 Job Retention Scheme Targeted by Scammers
* Government Offers Startups Â£500m Funding Option
* Thales Tech to Secure Motorola's New eSIM RAZR Smartphone
* ICO Gives Cautious Thumbs-Up to #COVID19 Contact Tracing Apps
* Hackers Raid Crypto Firms in $25m Attacks
* Trickbot Named Most Prolific #COVID19 Malware
* UK Tax Refund Email Scam Uncovered
* Hartford HealthCare Hit by Valentine's Day Data Breach
* FCC Gives Ligado's L-Band 5G Proposal the Thumbs Up
* Google: We Block 240 Million Daily #COVID19 Spam Messages
* Zoom Brings Renowned Crypto and Bug Bounty Experts on Board

Naked Security

* Maze ransomware hits US giant Cognizant
* Fan vibrations can be used to transmit data from air-gapped machines
* New sextortion scam: "High level of risk. Your account has been hacked."
* Bot creates millions of fake eyeballs to rip off smart-TV advertisers
* Monday review - the hot 13 stories of the week
* Critical bug in Google Chrome - get your update now
* US offers up to $5m reward for information on North Korean hackers
* GitHub users targeted by Sawfish phishing campaign
* TikTok announces "Family Pairing" - bust your moves but cap the risk
* S2 Ep35: TikTok woes, sextortion scams and passwords vs. single sign-on - Naked Security Podcast

Quick Heal - Security Simplified

* How safe it is to use the Zoom video-conferencing app?
* Beware of scams during this crucial time of CoronaVirus pandemic
* Dharma Ransomware Variant Malspam Targeting COVID-19
* Android application found on Google Play Store carrying Windows malware!
* Is the Coronavirus becoming an attack channel for ransomware?
* How can 1.33 billion people embrace digitalization in an era of damaging malware?
* Fake Coronavirus tracking app exploiting our fear and vulnerable social situation
* Are you secured when dealing with money on your mobile phones?
* CVE-2020-0796 - A "wormable" Remote Code Execution vulnerability in SMB v3
* Can playing video games on the PC cause cyberattacks?

Threat Post

* Bitcoin Stealers Hide in 700+ Ruby Developer Libraries
* DHS Urges Pulse Secure VPN Users To Update Passwords
* Attacks on Linksys Routers Trigger Mass Password Reset
* Zoom Bombing Attack Hits U.S. Government Meeting
* Hackers Update Age-Old Excel 4.0 Macro Attack
* Poorly Secured Docker Image Comes Under Rapid Attack
* New PoetRAT Hits Energy Sector With Data-Stealing Tools
* Cisco IP Phone Harbors Critical RCE Flaw
* Streaming TV Fraudsters Steal Millions of Ad Dollars in 'ICEBUCKET' Attack
* Alleged Zoom Zero-Days for Windows, MacOS for Sale, Report

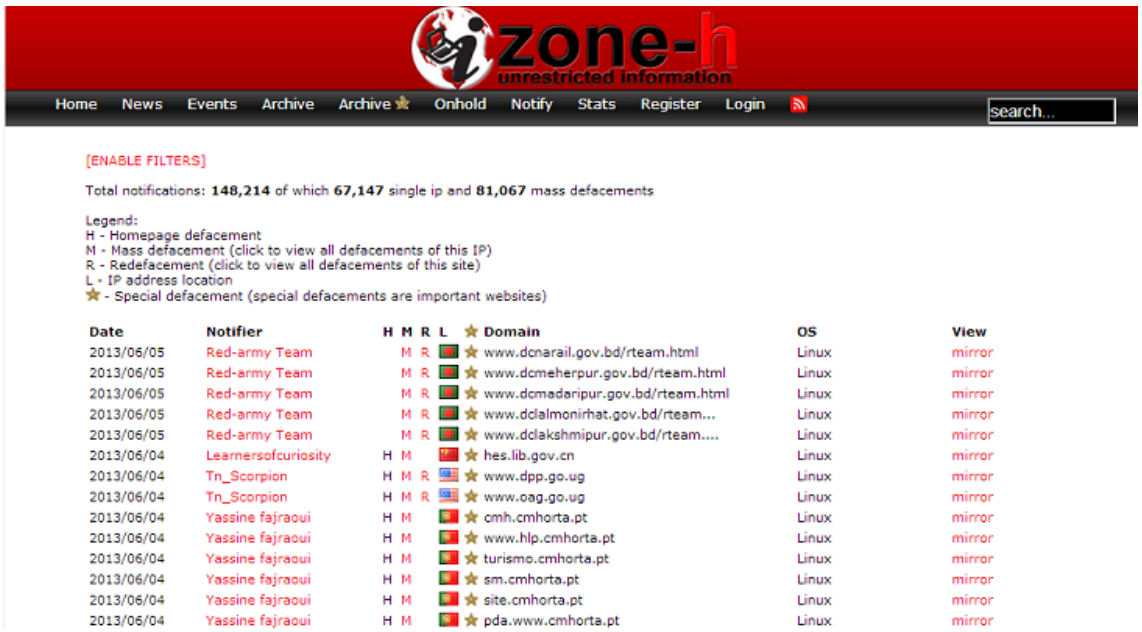
The Hacker Corner

Conferences

* Cybersecurity Podcasts (With Categories)
* Available Jobs During The Pandemic
* How To Convert Your Physical Conference To Online
* Soft 404
* Canceled Cyber Security Conferences
* 5 Tips To Help You Become A Better Public Speaker
* How To Get Public Cybersecurity Speaking Engagements
* Free Cybersecurity Conferences
* EC Council Training Courses 2020
* Advertising Landing Page Copy/Form

Latest Website Defacements

Unfortunately, at the time of this report, the resource was not availible.
You can access this resourse here: http://www.zone-h.org/rss/specialdefacements



Tools & Techniques

Packet Storm Security Tools Links

* Falco 0.22.1
* Packet Fence 10.0.0
* Zeek 3.1.2
* TestSSL 3.0.1
* nfstream 4.0.0
* SkyWrapper Discovery Tool
* Wireshark Analyzer 3.2.3
* Mandos Encrypted File System Unattended Reboot Utility 1.8.11
* netABuse Insufficient Windows Authentication Logic Scanner
* SQLMAP - Automatic SQL Injection Tool 1.4.4

Kali Linux Tutorials

* Domained : Multi Tool Subdomain Enumeration
* Lollipopz : Data Exfiltration Utility For Testing Detection Capabilities
* Sherloq : An Open-Source Digital Image Forensic Toolset
* Privacy Badger : A Browser Extension Automatically Learns To Block Invisible Trackers
* Audix : A PowerShell Tool To Quickly Configure Windows Event
* Serverless-Prey : Serverless Functions For Establishing Reverse Shells
* How to Install Metasploitable3 on Windows 10
* Lunar : A Lightweight Native DLL Mapping Library
* Ps-Tools : An Advanced Process Monitoring Toolkit For Offensive Operations
* Eavesarp : Analyze ARP Requests To Identify Intercommunicating Hosts

GBHackers Analysis

* TikTok Vulnerability Let Hackers to Hijack any Video Content
* Oracle Critical Patch Update Addresses 405 New Security Vulnerabilities - April 2020
* Critical VMware Flaw Let Attackers to Hack VMware vCenter Server
* iOS/macOS Webcam Can be Hacked With A Single Click On Malformed Link - Hacker Rewarded $75,000
* Critical Zoom Vulnerability Allows Hackers to Steal your Windows Password & Escalate Privileges with

CSI Linux

A Linux Distro focusing on Online Investigations and Incident Response. Download here.
Help grow the distribution by giving feedback and suggestions.

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Centreon 19.10.5 SQL Injection
* Xinfire DVD Player 5.5.0.0 Buffer Overflow
* Xinfire TV Player 6.0.1.2 Buffer Overflow
* Nsauditor 3.2.1.0 Buffer Overflow
* ALLPlayer 7.6 Buffer Overflow
* Atomic Alarm Clock 6.3 Stack Overflow
* Rubo DICOM Viewer 2.0 Buffer Overflow
* Atomic Alarm Clock 6.3 Unquoted Service Path
* Oracle Solaris 11.x / 10 whodo / w Buffer Overflow
* Common Desktop Environment 2.3.1 / 1.6 libDtSvc Buffer Overflow
* Common Desktop Environment 1.6 Local Privilege Escalation
* Fork CMS 5.8.0 Script Insertion
* Swift File Transfer Mobile Cross Site Scripting / Information Disclosure
* Prestashop 1.7.6.4 XSS / CSRF / Remote Code Execution
* Unraid 6.8.0 Authentication Bypass / Arbitrary Code Execution
* Metasploit Libnotify Arbitrary Command Execution
* SMACom 1.2.0 Insecure Transit / Password Disclosure
* TAO Open Source Assessment Platform 3.3.0 RC02 Cross Site Scripting
* Code Blocks 16.01 Buffer Overflow
* Playable 9.18 Script Insertion / Arbitrary File Upload
* Cisco IP Phone 11.7 Denial Of Service
* Easy MPEG To DVD Burner 1.7.11 Buffer Overflow
* Microsoft Windows Unquoted Service Path Privilege Escalation
* Nexus Repository Manager 3.21.1-01 Remote Code Execution
* TP-Link Archer A7/C7 Unauthenticated LAN Remote Code Execution

CXSecurity

* Nexus Repository Manager 3.21.1-01 Remote Code Execution
* Metasploit Libnotify Arbitrary Command Execution
* Unraid 6.8.0 Authentication Bypass / Arbitrary Code Execution
* Apache Solr Remote Code Execution via Velocity Template (Metasploit)
* Code Blocks 16.01 Buffer Overflow
* Liferay Portal Java Unmarshalling Remote Code Execution
* TP-Link Archer A7/C7 Unauthenticated LAN Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

* [remote] Apache Solr - Remote Code Execution via Velocity Template (Metasploit)
* [local] VMware Fusion - USB Arbitrator Setuid Privilege Escalation (Metasploit)
* [remote] DotNetNuke - Cookie Deserialization Remote Code Execution (Metasploit)
* [remote] PlaySMS - index.php Unauthenticated Template Injection Code Execution (Metasploit)
* [remote] Pandora FMS - Ping Authenticated Remote Code Execution (Metasploit)
* [remote] ThinkPHP - Multiple PHP Injection RCEs (Metasploit)
* [remote] Liferay Portal - Java Unmarshalling via JSONWS RCE (Metasploit)
* [remote] TP-Link Archer A7/C7 - Unauthenticated LAN Remote Code Execution (Metasploit)
* [local] BlazeDVD 7.0.2 - Buffer Overflow (SEH)
* [webapps] Xeroneit Library Management System 3.0 - 'category' SQL Injection
* [webapps] File Transfer iFamily 2.1 - Directory Traversal
* [webapps] DedeCMS 7.5 SP2 - Persistent Cross-Site Scripting
* [webapps] Macs Framework 1.14f CMS - Persistent Cross-Site Scripting
* [webapps] SeedDMS 5.1.18 - Persistent Cross-Site Scripting
* [webapps] Pinger 1.0 - Remote Code Execution
* [webapps] SuperBackup 2.0.5 for iOS - Persistent Cross-Site Scripting
* [webapps] AirDisk Pro 5.5.3 for iOS - Persistent Cross-Site Scripting
* [webapps] Oracle WebLogic Server 12.2.1.4.0 - Remote Code Execution
* [webapps] WSO2 3.1.0 - Persistent Cross-Site Scripting
* [webapps] Edimax Technology EW-7438RPn-v3 Mini 1.27 - Remote Code Execution
* [local] B64dec 1.1.2 - Buffer Overflow (SEH Overflow + Egg Hunter)
* [webapps] MOVEit Transfer 11.1.1 - 'token' Unauthenticated SQL Injection
* [webapps] Wordpress Plugin Media Library Assistant 2.81 - Local File Inclusion
* [local] Free Desktop Clock x86 Venetian Blinds Zipper 3.0 - Unicode Stack Overflow (SEH)
* [webapps] WSO2 3.1.0 - Arbitrary File Delete

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.

Cyber Security Video Channels

Black Hat

* CyberWire office tour with Dave: week 5
* DATATRIBE TOUR WITH DAVE
* evm: ALLSTAR: New Challenge Problems for Static Analysis
* Patrick Wardle: Making the Old, New: repurposing macOS malware

Defcon Conference

* Bridge Attack Double edged Sword in MobileSec - Zidong Han - DEF CON China 1
* Breaking the back end! - Gregory Pickett - DEF CON China 1
* Creating the DEFCON China 1.0 Badge - Joe Grand - DEF CON China 1
* Hacking Driverless Vehicles - Zoz - DEF CON China 1

Hack5

* ThreatWire 2020 04 14
* Hacking an Xbox Chatpad into a QWERTY Phone Case
* Wiping MBRs with COVID-19 Malware - ThreatWire
* How Hackers Are Helping Fight Coronavirus - ThreatWire

The PC Security Channel [TPSC]

* Windows Defender Hardening and Test vs Malware
* NordLocker Review: Encryption vs Ransomware?
* ESET Internet Security vs Ransomware
* Avast Test vs Ransomware

Eli the Computer Guy

* PHP - isset() Function to Verify if a Variable Has a Value
* PHP - $SESSION Variables
* PHP - $_GET to Send Variables in Hyperlinks
* PHP Project - Edit Picture Data in Gallery with MySQL Backend

Security Now

* Virus Contact Tracking - Security Now 762
* Zoom Go Boom - Security Now 761

Troy Hunt

* Weekly Update 187

Advisories

US-Cert Alerts & bulletins

* Apple Releases Security Update for Xcode
* Google Releases Security Updates
* Cisco Releases Security Updates for Multiple Products
* Oracle Releases April 2020 Security Bulletin
* VMware Releases Security Updates for vRealize Log Insight
* Intel Releases Security Updates
* Microsoft Releases April 2020 Security Updates
* Adobe Releases Security Updates for Multiple Products
* AA20-107A: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching
* AA20-106A: Guidance on the North Korean Cyber Threat
* AA20-099A: COVID-19 Exploited by Malicious Cyber Actors
* Vulnerability Summary for the Week of April 6, 2020
* Vulnerability Summary for the Week of March 30, 2020
* Vulnerability Summary for the Week of March 23, 2020

Symantec - Latest Threats

Unfortunately, at the time of this report, the resource was not availible.

Symantec - Latest Risk

Unfortunately, at the time of this report, the resource was not availible.

Advisories

Symantec - Latest Advisories

Unfortunately, at the time of this report, Symantec advisories was not availible.

NCSC - Latest Advisories

Weekly Threat Report 17th April 2020
The NCSC's weekly threat report is drawn from recent open source reporting.
Weekly Threat Report 10th April 2020
The NCSC's weekly threat report is drawn from recent open source reporting.

Zero Day Initiative Advisories

ZDI-CAN-10849: FreeBSD
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 'Vishnu' was reported to the affected vendor on: 2020-04-17, 3 days ago. The vendor is given until 2020-08-15 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-10756: IBM
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'tint0' was reported to the affected vendor on: 2020-04-17, 3 days ago. The vendor is given until 2020-08-15 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-10749: IBM
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 'tint0' was reported to the affected vendor on: 2020-04-17, 3 days ago. The vendor is given until 2020-08-15 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-10732: IBM
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 'b0yd' was reported to the affected vendor on: 2020-04-17, 3 days ago. The vendor is given until 2020-08-15 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-10790: Trend Micro
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 '@Kharosx0' was reported to the affected vendor on: 2020-04-16, 4 days ago. The vendor is given until 2020-08-14 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-10962: Microsoft
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 'Abdul-Aziz Hariri of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-04-15, 5 days ago. The

vendor is given until 2020-08-13 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-10667: Delta Industrial Automation

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 'Justin Taft (@oneupsecurity) and Chris Anastasio (@mufinnnnnnn)' was reported to the affected vendor on: 2020-04-15, 5 days ago. The vendor is given until 2020-08-13 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-10502: Marvell

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 'rgod' was reported to the affected vendor on: 2020-04-15, 5 days ago. The vendor is given until 2020-08-13 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-10836: Microsoft

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10833: Apple

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 'Junzhi Lu(@pwn0rz), Todd Han and Lilang Wu of Trend Micro' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10795: 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 'Reno Robert' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10762: 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 'Conor McErlane' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10605: Schneider Electric

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 'rgod' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10604: Schneider Electric

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 'rgod' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10603: Hewlett Packard Enterprise

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10602: Hewlett Packard Enterprise

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was

reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10601: Hewlett Packard Enterprise

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 'rgod' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10515: Trend Micro

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 '@Kharosx0' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10111: Apple

A CVSS score 7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by '0011' was reported to the affected vendor on: 2020-04-14, 6 days ago. The vendor is given until 2020-08-12 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-10936: Microsoft

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 'Abdul-Aziz Hariri of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-04-13, 7 days ago. The vendor is given until 2020-08-11 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-10935: Microsoft

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 'Abdul-Aziz Hariri of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-04-13, 7 days ago. The vendor is given until 2020-08-11 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-10890: Delta Industrial Automation

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 'kimiya' was reported to the affected vendor on: 2020-04-09, 11 days ago. The vendor is given until 2020-08-07 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-10889: Delta Industrial Automation

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: 2020-04-09, 11 days ago. The vendor is given until 2020-08-07 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-10886: Delta Industrial Automation

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-04-09, 11 days ago. The vendor is given until 2020-08-07 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-4331-1

Ubuntu Security Notice 4331-1 - A large number of security issues were discovered in the WebKitGTK+ Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

CA API Developer Portal 4.2.x / 4.3.1 Access Bypass / Privilege Escalation

CA Technologies, A Broadcom Company, is alerting customers to multiple vulnerabilities in CA API Developer Portal. Multiple vulnerabilities exist that can allow attackers to bypass access controls, view or modify sensitive information, perform open redirect attacks, or elevate privileges. CA published solutions to address these vulnerabilities and recommends that all affected customers implement these solutions. Versions 4.2.x and below along with 4.3.1 are affected.

Red Hat Security Advisory 2020-1497-01

Red Hat Security Advisory 2020-1497-01 - Virtual Network Computing is a remote display system which allows users to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2020-1495-01

Red Hat Security Advisory 2020-1495-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.7.0. Issues addressed include out of bounds write and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-1496-01

Red Hat Security Advisory 2020-1496-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.7.0. Issues addressed include out of bounds write and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-1493-01

Red Hat Security Advisory 2020-1493-01 - The kernel-alt packages provide the Linux kernel version 4.x. Issues addressed include buffer overflow, denial of service, heap overflow, and null pointer vulnerabilities.

Red Hat Security Advisory 2020-1488-01

Red Hat Security Advisory 2020-1488-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.7.0. Issues addressed include out of bounds write and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-1489-01

Red Hat Security Advisory 2020-1489-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.7.0. Issues addressed include out of bounds write and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-1487-01

Red Hat Security Advisory 2020-1487-01 - Chromium is an open-source web browser, powered by WebKit. This update upgrades Chromium to version 81.0.4044.92. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2020-1486-01

Red Hat Security Advisory 2020-1486-01 - The ipmitool packages contain a command-line utility for interfacing with devices that support the Intelligent Platform Management Interface specification. IPMI is an open standard for machine health, inventory, and remote power control. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-4330-1

Ubuntu Security Notice 4330-1 - It was discovered that PHP incorrectly handled certain file uploads. An attacker could possibly use this issue to cause a crash. It was discovered that PHP incorrectly handled certain PHAR archive files. An attacker could possibly use this issue to access sensitive information. It was discovered

that PHP incorrectly handled certain EXIF files. An attacker could possibly use this issue to access sensitive information or cause a crash. Various other issues were also addressed.

CA API Developer Portal 4.2.x / 4.3.1 Access Bypass / Privilege Escalation

CA Technologies, A Broadcom Company, is alerting customers to multiple vulnerabilities in CA API Developer Portal. Multiple vulnerabilities exist that can allow attackers to bypass access controls, view or modify sensitive information, perform open redirect attacks, or elevate privileges. CA published solutions to address these vulnerabilities and recommends that all affected customers implement these solutions. Versions 4.2.x and below as well as 4.3.1 are affected.

Kernel Live Patch Security Notice LSN-0065-1

Andrew Honig reported a flaw in the way KVM (Kernel-based Virtual Machine) emulated the IOAPIC. A privileged guest user could exploit this flaw to read host memory or cause a denial of service (crash the host). It was discovered that the KVM implementation in the Linux kernel, when paravirtual TLB flushes are enabled in guests, the hypervisor in some situations could miss deferred TLB flushes or otherwise mishandle them. An attacker in a guest VM could use this to expose sensitive information (read memory from another guest VM). Al Viro discovered that the vfs layer in the Linux kernel contained a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory).

Ubuntu Security Notice USN-4329-1

Ubuntu Security Notice 4329-1 - Felix Wilhelm discovered that Git incorrectly handled certain URLs that included newlines. A remote attacker could possibly use this issue to trick Git into returning credential information for a wrong host.

Red Hat Security Advisory 2020-1478-01

Red Hat Security Advisory 2020-1478-01 - Red Hat JBoss Enterprise Application Platform is a platform for Java applications based on the JBoss Application Server. This asynchronous patch is a security update for the Apache Tomcat package in JBoss Enterprise Application Platform 6.4 for Red Hat Enterprise Linux 5, 6, and 7. All users of Red Hat JBoss Enterprise Application Platform 6.4 are advised to upgrade to this updated package.

Red Hat Security Advisory 2020-1479-01

Red Hat Security Advisory 2020-1479-01 - Red Hat JBoss Enterprise Application Platform is a platform for Java applications based on the JBoss Application Server. This asynchronous patch is a security update for the Apache Tomcat package in JBoss Enterprise Application Platform 6.4 for Red Hat Enterprise Linux 5, 6, and 7. All users of Red Hat JBoss Enterprise Application Platform 6.4 are advised to upgrade to these updated packages.

Red Hat Security Advisory 2020-1475-01

Red Hat Security Advisory 2020-1475-01 - Red Hat CodeReady Workspaces 2.1.0 provides a cloud developer-workspace server and a browser-based IDE built for teams and organizations. CodeReady Workspaces runs in OpenShift and is well-suited for container-based development. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2020-1465-01

Red Hat Security Advisory 2020-1465-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2020-1461-01

Red Hat Security Advisory 2020-1461-01 - The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. Issues addressed include an out of bounds write vulnerability.

Red Hat Security Advisory 2020-1471-01

Red Hat Security Advisory 2020-1471-01 - The elfutils packages contain a number of utility programs and libraries related to the creation and maintenance of executable code. A double-free issue was addressed.

Red Hat Security Advisory 2020-1470-01

Red Hat Security Advisory 2020-1470-01 - The Network Time Protocol is used to synchronize a computer's

time with another referenced time source. These packages include the ntpd service which continuously adjusts system time and utilities used to query and configure the ntpd service. Issues addressed include buffer overflow, code execution, and denial of service vulnerabilities.

Red Hat Security Advisory 2020-1464-01

Red Hat Security Advisory 2020-1464-01 - The procps-ng packages contain a set of system utilities that provide system information, including ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch, and pwdx. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2020-1462-01

Red Hat Security Advisory 2020-1462-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2020-1396-01

Red Hat Security Advisory 2020-1396-01 - The podman tool manages Pods, container images, and containers. It is part of the libpod library, which is for applications that use container Pods. Container Pods is a concept in Kubernetes. A file overwrite issue was addressed.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com