CYBER WAR

WEEKLY AWARENESS REPORT

04-27-20

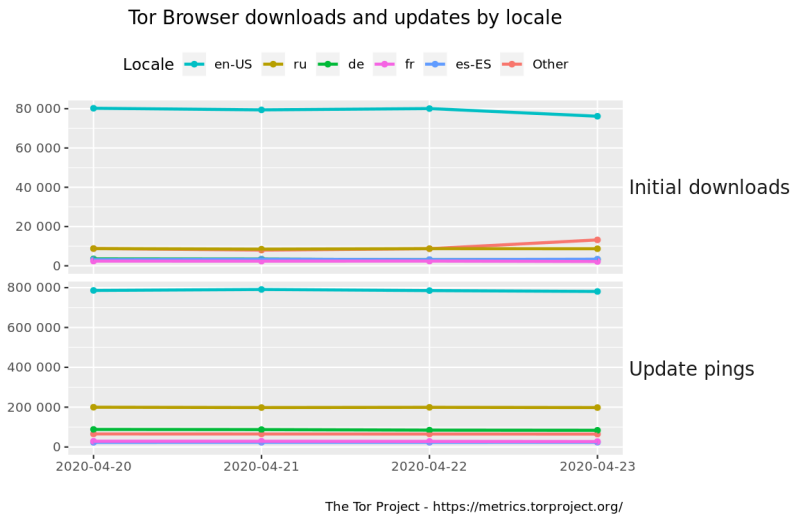
April 27, 2020

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

* UK Spies Will Need Artificial Intelligence
* Israel Government Tells Water Treatment Companies To Change Passwords
* Microsoft Teams Could Be Pwned With A Gif
* New iOS Text Bomb Bug Can Crash Your iPhone
* 160,000 Nintendo Accounts Were Compromised
* Apple Disputes Recent iOS Zero Day Claim
* Georgia Reopens Businesses As Death Toll Rises
* A Dozen Nation Backed APTs Tap COVID-19 To Cover Spy Attacks
* Valve Confirms CS:GO, Team Fortress 2 Source Code Leak
* ESET Takes Down VictoryGate Cryptomining Botnet
* NSA Shares List Of Vulnerabilities Commonly Exploited To Plant Web Shells
* Zero-Click, Zero-Day Flaws In iOS Mail Used In Targeted VIP Attacks
* Hackers Have Breached 60 Ad Servers To Load Their Own Malicious Ads
* Small Businesses Tapping COVID-19 Loans Hit With Data Exposure
* Coronavirus: Health Leaders Credentials Dumped Online
* Vietnam-Linked Hackers Targeted Chinese Government
* How To Hack A Company By Circumventing Its WAF For Fun And Profit - Part 2
* The CFAA Is Finally Being Reviewed By The Supreme Court
* DForce Hacker Returns $25m In Stolen Cryptocurrency
* Nintendo Accounts Are Getting Hacked To Buy Fortnite Currency
* Hackers Target Oil Producers With Attacks
* 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

Krebs on Security

* Unproven Coronavirus Therapy Proves Cash Cow for Shadow Pharmacies
* When in Doubt: Hang Up, Look Up, & Call Back
* Who's Behind the "Reopen" Domain Surge?
* 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

Dark Reading

* COVID-19 Quarantine: A Unique Learning Opportunity for Defenders
* COVID-19: Latest Security News & Commentary
* Health Prognosis on the Security of IoMT Devices? Not Good
* WHO Confirms Email Credentials Leak
* MSI Utility Vulnerability Based on Missing Quotation Marks
* Apple Downplays Threat Posed by Newly Disclosed Zero-Days in iOS
* Cybercrime Group Steals $1.3M from Banks
* Find Your Framework: Thinking Fast and Slow
* Sextortion Campaigns Net Cybercriminals Nearly $500K in Five Months
* Narrow the Scope of Compliance
* Paay Misconfiguration Leaves Transaction Data Exposed
* Why Consumers, SMBs Are Likely to Fall for Coronavirus Scams
* 5 Ways to Prove Security's Worth in the Age of COVID-19
* How the Dark Web Fuels Insider Threats
* Communication, Cloud & Finance Apps Most Vulnerable to Insider Threat
* Resiliency: The Trait National Sporting Leagues Share with Security & IT Teams
* Demand for Cybersecurity Jobs Declines But Still Outperforms Other Sectors
* White-Hat Hackers Help 'Fold' COVID-19 Proteins
* The Evolving Threat of Credential Stuffing
* Attackers Prefer Ransomware to Stealing Data

The Hacker News

* How An Image Could've Let Attackers Hack Microsoft Teams Accounts
* Malicious USB Drives Infect 35,000 Computers With Crypto-Mining Botnet
* Hackers Trick 3 British Private Equity Firms Into Sending Them $1.3 Million
* Zero-Day Warning: It's Possible to Hack iPhones Just by Sending Emails
* Chinese Hackers Using New iPhone Hack to Spy On Uyghur Muslims
* The Incident Response Challenge 2020 - Win $5,000 Prize!
* Researcher Discloses 4 Zero-Day Bugs in IBM's Enterprise Security Software
* Unpatchable 'Starbleed' Bug in FPGA Chips Exposes Critical Devices to Hackers
* 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

Security Week

* Iran Paper Accuses US of Stealing Its .Com
* Critical Ignition Gateway Vulnerability Can Lead to Disruption in Plants
* FCC Only Partially Improved Its Cybersecurity Posture, GAO Says
* Israel Says Hackers Targeted SCADA Systems at Water Facilities
* Collection of South Korean, U.S. Payment Cards Emerges on Underground Market
* Kaspersky and SecurityWeek Present SAS@home Virtual Event - April 28-30
* Microsoft Teams Vulnerability Exposed Organizations to Attacks
* Malware Delivered to Sophos Firewalls via Zero-Day Vulnerability
* Intelligence Agencies Share Web Shell Detection Techniques
* Flaws in ABB DCS Allow Hackers to Cause Disruption in Industrial Environments
* 'VictoryGate' Botnet Infected 35,000 Devices via USB Drives
* Apple Finds No Evidence of Attacks Targeting iOS Mail App Vulnerabilities
* New GreyNoise Service Alerts Organizations of Compromised Networks
* Hoaxcalls Botnet Expands Targets List, DDoS Capabilities
* Mozilla Offers Bigger Rewards for Firefox Vulnerabilities
* Malwarebytes Unveils New Privacy VPN Service
* Automated Red Teaming Firm Randori Raises $20 Million
* Nazar: Old Iran-Linked APT Operation Monitored by NSA
* Rapid Change is the New Normal
* Vietnamese Hackers Mount COVID-19 Espionage Campaigns Against China

Infosecurity Magazine

* 89% Reduction in Removal of Child Sexual Abuse Webpages During #COVID19
* Online Safety Tech Industry Association Launches
* #COVID19 Fallout Hits UK Tech Startups Hard as Confidence Slumps
* Nintendo Breach Affects 160,000 User Accounts
* Experts Detect 30,000% Increase in #COVID19 Threats
* Piracy Site Popcorn Time Targets Kids with New Version
* Australian Police Rescue Children from Online Pornography Ring
* Anti-bullying Group Asks Families to Discuss Cyber-bullying
* UK Citizens Urged to Limit Screen Time During Lockdown
* Information and Data Sharing Crucial in #COVID19 Efforts
* Google Tackles Fake Ads as #COVID19 Counterfeits Surge
* Twitter Moves to Ban 5G #COVID19 Conspiracy Theories

Naked Security

* 5 common mistakes that lead to ransomware
* Web shell warning issued by US and Australia
* Monday review - the hot 16 stories of the week
* Patch now! Microsoft issues unexpected Office fix
* Shadow Broker leaked NSA files point to unknown APT group
* AI helps experts find thousands of child sexual abuse imagery keywords
* iPhone zero day - don't panic! Here's what you need to know
* Trove of RubyGems malware highlights software supply chain issues
* Password-free database of exercise app Kinomap leaks 42m user records
* S2 Ep36: Rogue Chrome extensions, Signal fears and Darth Vader - Naked Security podcast

Quick Heal - Security Simplified

* Coronavirus-themed Campaign delivers Agent Tesla Malware
* Way Out of The MAZE: A Quick Guide For Defending Against Maze Ransomware
* 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?

Threat Post

* Hackers Mount Zero-Day Attacks on Sophos Firewalls
* U.S. Universities Hit With 'Adult Dating' Spear-Phishing Attack
* Eight Common OT / Industrial Firewall Mistakes
* Single Malicious GIF Opened Microsoft Teams to Nasty Attack
* SAS@home Virtual Summit Showcases New Threat Intel, Industry Changes
* Latest Apple Text-Bomb Crashes iPhones via Message Notifications
* News Wrap: Nintendo Account Hacks, Apple Zero Days, NFL Security
* Nintendo Confirms Breach of 160,000 Accounts
* Apple Pushes Back Against Zero-Day Exploit Claims
* Valve Confirms CS:GO, Team Fortress 2 Source-Code Leak

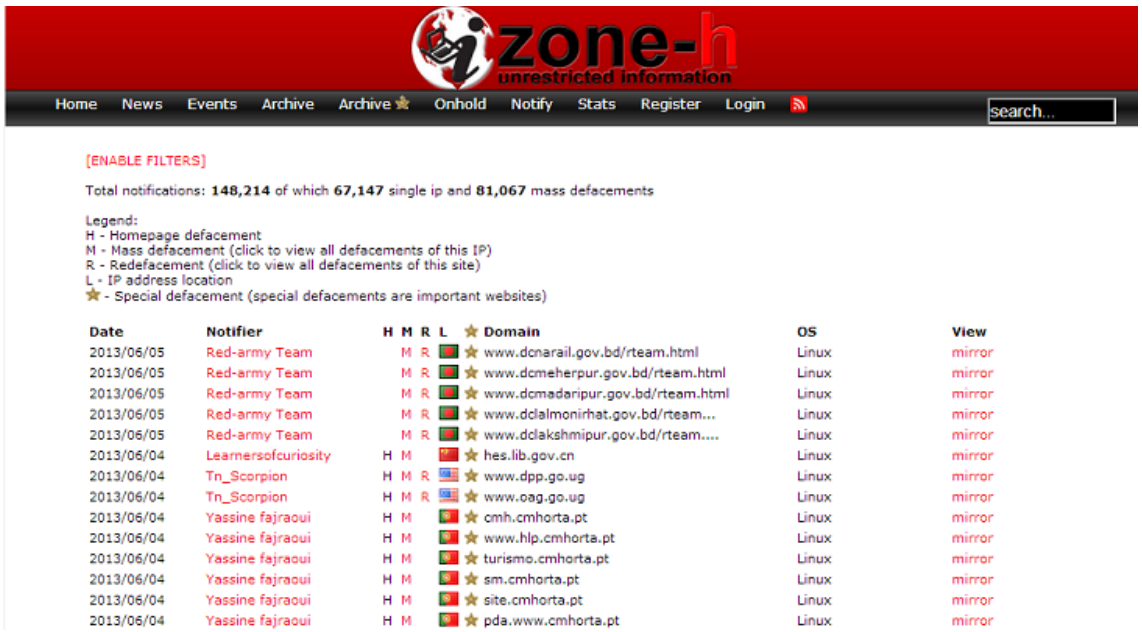
The Hacker Corner

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

* Bing.com Hostname / IP Enumerator 1.0.2
* URLCrazy Domain Name Typo Tool 0.7.1
* nfstream 4.0.1
* Faraday 3.11
* OpenSSL Toolkit 1.1.1g
* Falco 0.22.1
* Packet Fence 10.0.0
* Zeek 3.1.2
* TestSSL 3.0.1
* nfstream 4.0.0

Kali Linux Tutorials

* Lulzbuster : A Very Fast & Smart Web Directory
* Impulse : Denial-of-service ToolKit
* NullScan : A Modular Framework Designed To Chain & Automate Security Tests
* GithubFind3r : Fast Command Line Repo/User/Commit Search Tool
* httpgrep : Scans HTTP Servers To Find Given Strings In URIs
* Adamantium-Thief : Decrypt Chromium Based Browsers Passwords & Credit Cards
* LK_Scraper : An Fully Configurable LinkedIn Scrape
* Flux-Keylogger : Modern Javascript Keylogger With Web Panel
* Vulnx : Auto Shell Injector That Detect Vulnerabilities In Multiple Types Of CMS
* pwndrop : Self-Deployable File Hosting Service

GBHackers Analysis

* Hackers Exploit SQL Injection & Code Execution Zero-day Bugs in Sophos Firewall
* Four IBM Zero-days Leaked Online After the Company Refused to Patch The Bugs
* 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

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

* Docker-Credential-Wincred.exe Privilege Escalation
* Geeklog 2.2.1 SQL Injection
* Maian Support Helpdesk 4.3 Cross Site Request Forgery
* Online Course Registration 2.0 SQL Injection
* Online Shopping System Advanced 1.0 SQL Injection
* Geeklog 2.2.1 Cross Site Scripting
* Netis E1+ 1.2.32533 Password Leak
* PHP-Fusion 9.03.50 Arbitrary File Upload
* Netis E1+ 1.2.32533 Hardcoded Backdoor Account
* Open-AudIT 3.3.0 Cross Site Scripting
* jQuery html() Cross Site Scripting
* Furukawa Electric ConsciusMAP 2.8.1 Java Deserialization Remote Code Execution
* Air Sender 1.0.2 Arbitrary File Upload
* Edimax EW-7438RPn 1.13 Remote Code Execution
* EspoCRM 5.8.5 Privilege Escalation
* Popcorn Time 6.2 Unquoted Service Path
* WebKit AudioArray::allocate Data Race / Out-Of-Bounds Access
* WebRTC Layer Info Out-Of-Bounds Write
* Chrome AudioArray::Allocate Data Race / Out-Of-Bounds Access
* WebRTC FEC Extension Processing Out-Of-Bounds Write
* Zen Load Balancer 3.10.1 Directory Traversal
* Complaint Management System 4.2 Cross Site Request Forgery
* Complaint Management System 4.2 SQL Injection
* AMD Radeon DirectX 11 Driver 8.17.10.0871 Memory Corruption
* Complaint Management System 4.2 Cross Site Scripting

CXSecurity

* Furukawa Electric ConsciusMAP 2.8.1 Java Deserialization Remote Code Execution
* AMD Radeon DirectX 11 Driver 8.17.10.0871 Memory Corruption
* VB 6.0 Dirlist Object - Code Execution
* NSClient++ 0.5.2.35 Authenticated Remote Code Execution
* Rubo DICOM Viewer 2.0 Buffer Overflow
* Xinfire TV Player 6.0.1.2 Buffer Overflow
* IQrouter 3.3.1 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

* Breaking the back end! - Gregory Pickett - DEF CON China 1
* Bridge Attack Double edged Sword in MobileSec - Zidong Han - DEF CON China 1
* Creating the DEFCON China 1.0 Badge - Joe Grand - DEF CON China 1
* Warning Magnitude 10 Earthquake Is Coming in One Minute - Weiguang Li - DEF CON China 1

Hack5

* Jailbreaking CPAP Machines To Be Ventilators - ThreatWire
* ThreatWire 2020 04 14
* Hacking an Xbox Chatpad into a QWERTY Phone Case
* Wiping MBRs with COVID-19 Malware - 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 Project - Simple Network Up Down Monitor (shell_exec)
* PHP - Send Shell Commands with shell_exec()
* PHP - Parse Filenames and Paths with pathinfo()
* PHP - Test Variable Against an Array with in_array()

Security Now

* The COVID Effect - Security Now 763
* Virus Contact Tracking - Security Now 762

Troy Hunt

* Weekly Update 188

Advisories

US-Cert Alerts & bulletins

* OpenSSL Releases Security Update
* Microsoft Releases Security Updates for Multiple Products
* Google Releases Security Updates for Chrome
* NSA, ASD Release Guidance for Mitigating Web Shell Malware
* IC3 Releases Alert on Extortion Email Scams
* Apple Releases Security Update for Xcode
* Google Releases Security Updates
* Cisco 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 20, 2020
* Vulnerability Summary for the Week of April 13, 2020
* Vulnerability Summary for the Week of April 6, 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

Video conferencing: new guidance for individuals and for organisations
Whether you're using it to work from home, or just catching up with friends and family, new guidance from the NCSC will help you to use video conferencing securely.
Video conferencing services: using them securely
How to set up and use video conferencing services, safely and securely

Zero Day Initiative Advisories

ZDI-CAN-10930: Fuji Electric
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: 2020-04-27, 0 days ago. The vendor is given until 2020-08-25 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-10995: Advantech
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 'KPC' was reported to the affected vendor on: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10994: Advantech
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 'KPC' was reported to the affected vendor on: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10993: Advantech
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 'KPC' was reported to the affected vendor on: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10992: Advantech
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 'KPC' was reported to the affected vendor on: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10991: Advantech
A CVSS score 9.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H) severity vulnerability discovered by 'KPC' was

reported to the affected vendor on: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10970: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10660: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10658: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10657: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10656: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10655: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10645: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10636: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10634: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10633: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10630: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10629: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10628: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10627: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10626: Advantech

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: 2020-04-24, 3 days ago. The vendor is given until 2020-08-22 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-10990: Advantech

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 'KPC' was reported to the affected vendor on: 2020-04-23, 4 days ago. The vendor is given until 2020-08-21 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-10989: Advantech

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'KPC' was reported to the affected vendor on: 2020-04-23, 4 days ago. The vendor is given until 2020-08-21 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-10988: Advantech

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'KPC' was reported to the affected vendor on: 2020-04-23, 4 days ago. The vendor is given until 2020-08-21 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

Gentoo Linux Security Advisory 202004-13

Gentoo Linux Security Advisory 202004-13 - Multiple vulnerabilities have been found in Git which might all allow attackers to access sensitive information. Versions less than 2.26.2 are affected.

Gentoo Linux Security Advisory 202004-12

Gentoo Linux Security Advisory 202004-12 - Multiple vulnerabilities have been found in Chromium and Google Chrome, the worst of which could allow remote attackers to execute arbitrary code. Versions less than 81.0.4044.122 are affected.

Red Hat Security Advisory 2020-1561-01

Red Hat Security Advisory 2020-1561-01 - Twisted is an event-based framework for internet applications. Twisted Web is a complete web server, aimed at hosting web applications using Twisted and Python, but fully able to serve static pages too. HTTP request smuggling vulnerabilities were addressed.

Ubuntu Security Notice USN-4338-1

Ubuntu Security Notice 4338-1 - Agostino Sarubbo discovered that re2c incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code.

Gentoo Linux Security Advisory 202004-11

Gentoo Linux Security Advisory 202004-11 - Multiple vulnerabilities have been found in Mozilla Firefox, the worst of which could result in the arbitrary execution of code. Versions less than 68.7.0 are affected.

Gentoo Linux Security Advisory 202004-10

Gentoo Linux Security Advisory 202004-10 - Multiple vulnerabilities were found in OpenSSL, the worst of which could allow remote attackers to cause a Denial of Service condition. Versions less than 1.1.1g are affected.

Ubuntu Security Notice USN-4337-1

Ubuntu Security Notice 4337-1 - It was discovered that OpenJDK incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service while processing a specially crafted regular expression. It was discovered that OpenJDK incorrectly handled class descriptors and catching exceptions during object stream deserialization. An attacker could possibly use this issue to cause a denial of service while processing a specially crafted serialized input. Various other issues were also addressed.

Red Hat Security Advisory 2020-1545-01

Red Hat Security Advisory 2020-1545-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-1449-01

Red Hat Security Advisory 2020-1449-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. A local file overwrite vulnerability was addressed.

Red Hat Security Advisory 2020-1543-01

Red Hat Security Advisory 2020-1543-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically. Issues addressed include information leakage and password leak vulnerabilities.

Red Hat Security Advisory 2020-1541-01

Red Hat Security Advisory 2020-1541-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically. Issues addressed include information leakage, password leak, and traversal vulnerabilities.

Red Hat Security Advisory 2020-1544-01

Red Hat Security Advisory 2020-1544-01 - Ansible is a simple model-driven configuration management,

multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically. Issues addressed include information leakage and password leak vulnerabilities.

Red Hat Security Advisory 2020-1542-01

Red Hat Security Advisory 2020-1542-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically. Issues addressed include information leakage, password leak, and traversal vulnerabilities.

Ubuntu Security Notice USN-4336-1

Ubuntu Security Notice 4336-1 - It was discovered that GNU binutils contained a large number of security issues. If a user or automated system were tricked into processing a specially-crafted file, a remote attacker could cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2020-1538-01

Red Hat Security Advisory 2020-1538-01 - The release of Red Hat AMQ Online 1.4.1 serves as a replacement for AMQ online 1.4.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked in the References.

Red Hat Security Advisory 2020-1515-01

Red Hat Security Advisory 2020-1515-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include denial of service and deserialization vulnerabilities.

Red Hat Security Advisory 2020-1516-01

Red Hat Security Advisory 2020-1516-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include denial of service and deserialization vulnerabilities.

Red Hat Security Advisory 2020-1517-01

Red Hat Security Advisory 2020-1517-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. Issues addressed include denial of service and deserialization vulnerabilities.

Red Hat Security Advisory 2020-1524-01

Red Hat Security Advisory 2020-1524-01 - 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 2020-1526-01

Red Hat Security Advisory 2020-1526-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a memory exhaustion vulnerability.

Red Hat Security Advisory 2020-1527-01

Red Hat Security Advisory 2020-1527-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a memory exhaustion vulnerability.

Ubuntu Security Notice USN-4335-1

Ubuntu Security Notice 4335-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, bypass same-origin restrictions, conduct cross-site scripting attacks, or execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2020-1513-01

Red Hat Security Advisory 2020-1513-01 - Git is a distributed revision control system with a decentralized

architecture. A credential leak vulnerability has been addressed.

Red Hat Security Advisory 2020-1518-01

Red Hat Security Advisory 2020-1518-01 - Git is a distributed revision control system with a decentralized architecture. A credential leak vulnerability has been addressed.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com