CYBER WAR

WEEKLY AWARENESS REPORT

02-24-20

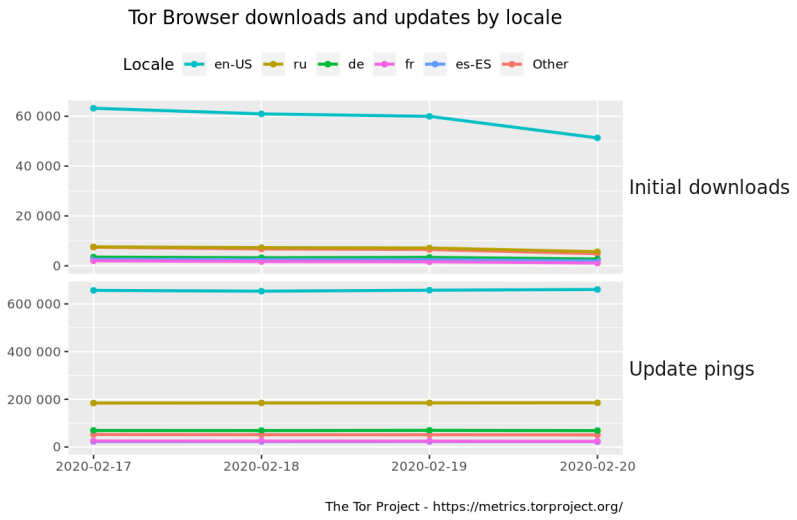
February 24, 2020

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

* CSI Linux Forensics Challenge

Using CSI Linux and the tools included, go through this forensic project and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner... Read the Cyber Intelligence Report 2020 Q1for 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

* Alexa Records You Up To 19 Times A day
* California Man Arrested For DDoS'ing Candidate's Website
* U.S. Lawmakers To Introduce Bill That Threatens Encryption On Tech Platforms
* Stone Gets 40 Months And A Rebuke From Judge For Lying To Congress
* Vendors Ditching RSA Over Coronavirus Fears
* Google Denies Harvesting Student Data With Free Chromebooks
* MGM Hack Exposes Personal Data Of 10.6 Million Guests
* ISS World Hack Leaves Thousands Of Employees Offline
* Adobe Releases Patch For Critical Code Execution Vulnerability
* US, UK Blame Russia For Mass Defacement Of Georgian Websites
* Australian MPs Call On UK To Block US Assange Extradition
* Ring Doorbell Makes Two Factor Verification Mandatory
* Chinese Hackers Have Breached Online Betting And Gambling Sites
* Why Rudy Giuliani's Twitter Typos Are A Security Fail
* IBM Pulls Out Of RSA Over Coronavirus Fears
* Hacker Scheme Threatens AdSense Customers
* Lenovo, HP, Dell Peripherals Face Unpatched Firmware Bugs
* 16 DDoS Attacks Take Place Every 60 Seconds, Rates Reach 622 Gbps
* Twitter Says Olympics, IOC Accounts Hacked
* Police Force Denies Creating Child Hacker Poster
* Hacking Brain-Computer Interfaces
* Signal Is Finally Bringing Its Secure Messaging To The Masses
* Privacy Experts Skeptical Of Proposed Data Protection Agency
* Black Hat Asia 2020 Postponed Due To Coronavirus Concerns
* Nedbank Says 1.7 Million Affected By Breach

Krebs on Security

* Zyxel Fixes 0day in Network Storage Devices
* Hackers Were Inside Citrix for Five Months
* Encoding Stolen Credit Card Data on Barcodes
* Pay Up, Or We'll Make Google Ban Your Ads
* A Light at the End of Liberty Reserve's Demise?
* Microsoft Patch Tuesday, February 2020 Edition
* U.S. Charges 4 Chinese Military Officers in 2017 Equifax Hack
* Dangerous Domain Corp.com Goes Up for Sale
* When Your Used Car is a Little Too 'Mobile'
* Booter Boss Busted By Bacon Pizza Buy

Dark Reading

* SSRF 101: How Server-Side Request Forgery Sneaks Past Your Web Apps
* Enterprise Cloud Use Continues to Outpace Security
* Solving the Cloud Data Security Conundrum
* Latest Security News from RSAC 2020
* 7 Tips to Improve Your Employees' Mobile Security
* All About SASE: What It Is, Why It's Here, How to Use It
* Emotet Malware Rears Its Ugly Head Again
* California Man Arrested for Politically Motivated DDoS
* NRC Health Ransomware Attack Prompts Patient Data Concerns
* Olympics Could Face Disruption from Regional Powers
* How to Get CISOs & Boards on the Same Page
* Security Now Merges With Dark Reading
* Popular Mobile Document-Management Apps Put Data at Risk
* Microsoft Announces General Availability of Threat Protection, Insider Risk Management
* Ransomware Damage Hit $11.5B in 2019
* It's Time to Break the 'Rule of Steve'
* Personal Info of 10.6M MGM Resort Guests Leaked Online
* 5 Strategies to Secure Cloud Operations Against Today's Cyber Threats
* 10 Tough Questions CEOs Are Asking CISOs
* Firms Improve Threat Detection but Face Increasingly Disruptive Attacks

The Hacker News

* Microsoft Brings Defender Antivirus for Linux, Coming Soon for Android and iOS
* Google Bans 600 Android Apps from Play Store for Serving Disruptive Ads
* Scam Alert: You've Been Selected for 'Like of the Year 2020' Cash Prizes
* Deal: Cloud And Networking Certification Training ~ Get 97% OFF
* Adobe Patches Critical Bugs Affecting Media Encoder and After Effects
* Ring Makes 2-Factor Authentication Mandatory Following Recent Hacks
* US Govt Warns Critical Industries After Ransomware Hits Gas Pipeline Facility
* Iranian Hackers Exploiting VPN Flaws to Backdoor Organizations Worldwide
* Cynet Offers Free Threat Assessment for Mid-sized and Large Organizations
* Critical Bug in WordPress Theme Plugin Opens 200,000 Sites to Hackers
* OpenSSH now supports FIDO U2F security keys for 2-factor authentication
* A Dozen Vulnerabilities Affect Millions of Bluetooth LE Powered Devices
* U.S. Charges Huawei with Stealing Trade Secrets from 6 Companies
* 500 Chrome Extensions Caught Stealing Private Data of 1.7 Million Users
* Download: Definitive 'IR Management and Reporting' Presentation Template

Security Week

* Vulnerabilities in Moxa Networking Device Expose Industrial Environments to Attacks
* Mismanagement of Device Identities Could Cost Businesses Billions: Report
* Canada Privacy Watchdog Probes Facial Recognition Startup
* Slickwraps Discloses Data Breach
* Cisco Unveils SecureX Security Platform
* Vulnerabilities Allow Hackers to Access Honeywell Fire Alarm Systems
* Man Tied to Ex-Congresswoman Campaign Arrested in Hack Spree
* 2016 Again? Russia Back to Stirring Chaos in U.S. Election
* New Mexico Sues Google Over Collection of Children's Data
* Google Removes 600 Android Apps for Displaying Disruptive Ads
* Malware Attack Takes ISS World's Systems Offline
* FireEye Spotted Over 500 New Malware Families in 2019
* VMware Patches Serious Flaws in vRealize Operations for Horizon Adapter
* U.S. Combat Support Agency Discloses 2019 Data Breach
* Fraudulent Login Attacks Against Banks Surge: Akamai
* 20,000 WordPress Websites Infected via Trojanized Themes
* Georgia Blames Russia for Cyberattack, US, UK Agree
* Cisco Patches Critical Flaw in Smart Licensing Solution
* Over 400 ICS Vulnerabilities Disclosed in 2019: Report
* RSAC 2020: Three Reasons Why the "Human Element" is a Timeless Theme

Infosecurity Magazine

* FBI Arrests Man on Political Cyber-attack Charges
* UW Medicine Facing Breach Lawsuit
* Tech Industry is the Least Secure Industry, Say Hackers
* Google Pulls 600 Apps from Play Store
* US Defense Agency Notifies Users of Serious Breach
* Over 120 Million US Consumers Exposed in Privacy Snafu
* US Cyber-flashers Could Get $1K Fine
* Booz Allen Awarded $113m SEC Contract
* New Jersey Hospital Network Faces Lawsuit Over Ransomware Attack
* GDPR Protection Will Continue After Google's US Data Move, Says Lawyer
* UK Names and Shames Russia for Georgia Cyber-Attacks
* MGM Customer Data Has Been on Dark Web for Six Months

Naked Security

* KidsGuard stalkerware leaks data on secretly surveilled victims
* Google purges 600 Android apps for "disruptive" pop-up ads
* Apple chops Safari's TLS certificate validity down to one year
* Monday review - the hot 25 stories of the week
* The Amazon Prime phishing attack that wasn't…
* S2 Ep27: Bluetooth holes, dodgy Chrome extensions and forgotten passwords - Naked Security Podcast
* Larry Tesler, of copy-and-paste fame, dies at 74
* US and UK call out Russian hackers for Georgia attacks
* Data of 10.6m MGM hotel guests posted for sale on Dark Web forum
* Adobe fixes critical flaws in Media Encoder and After Effects

Quick Heal - Security Simplified

* Take your browser security to the next level!
* Ouroboros: Following A New Trend In Ransomware League
* A Deep Dive Into Wakeup On Lan (WoL) Implementation of Ryuk
* Hackers are riding on the global panic pertaining to the deadly Coronavirus
* Unable to Shut down or Restart Windows 7 systems?
* Why secure your IoT Devices?
* HorseDeal Riding on The Curveball!
* A sloppy click can exfiltrate your important data!
* New wave of Mal-Spam campaign attaching Disk Imaging Files
* Ako Ransomware targeting businesses using RaaS

Threat Post

* Data Breach Occurs at Agency in Charge of Secure White House Communications
* Lawsuit Claims Google Collects Minors' Locations, Browsing History
* Active Attacks Target Popular Duplicator WordPress Plugin
* RSAC 2020: Editors' Preview of Hottest Sessions, Speakers and Themes
* Burning Man Tickets for $225? Yep, Too Good to Be True
* ISS World Hit with Malware Attack that Shuts Down Global Computer Network
* New 'Haken' Malware Found On Eight Apps In Google Play Store
* Google Bans 600 Android Apps for Obnoxious Ads
* Critical Cisco Bug Opens Software Licencing Manager to Remote Attack
* Cybergang Favors G Suite and Physical Checks For BEC Attacks

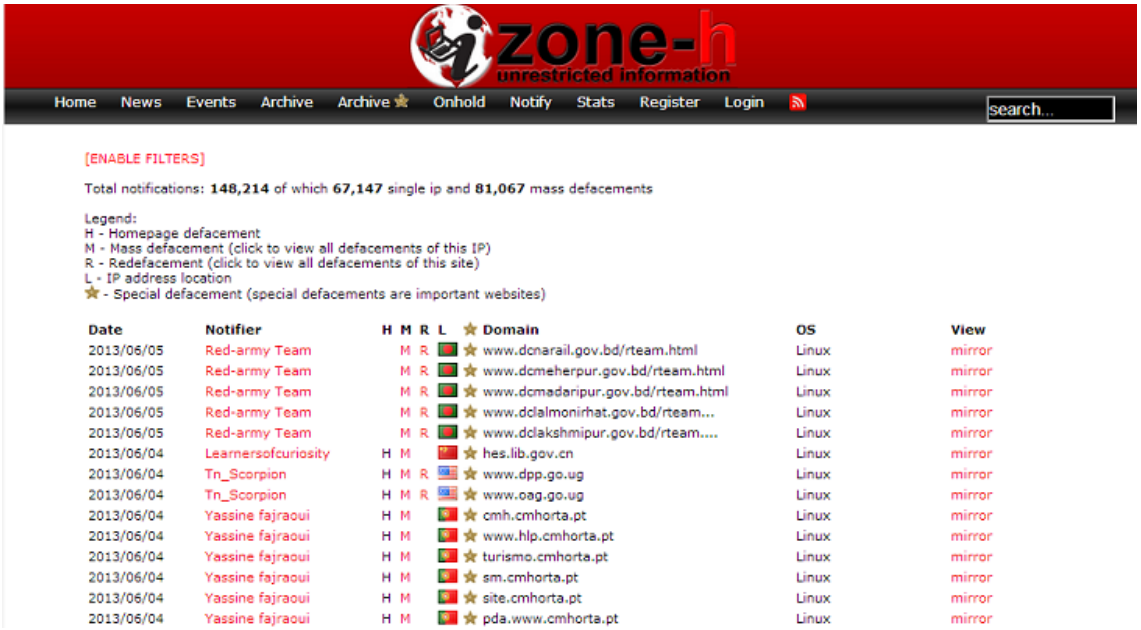
The Hacker Corner

Conferences

* Free Cybersecurity Conferences
* EC Council Training Courses 2020
* Advertising Landing Page Copy/Form
* Apply: FREE 6 Month InfoSec Speaking Plan
* Apply: FREE 30 Day InfoSec Speaking Plan
* How To Speak At DEF CON
* Join Our LinkedIn Group
* Upcoming Cybersecurity Conferences in the United States & Canada
* Upcoming Cybersecurity Conferences in Europe
* 29 Amazing TED Cybersecurity Talks (2008 - 2020)

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

* Wapiti Web Application Vulnerability Scanner 3.0.3
* nfstream 3.2.0
* OpenDNSSEC 2.1.6
* Lulzbuster 1.2.0
* OpenSSH 8.2p1
* EnumJavaLibs Java Classpath Enumerator
* Suricata IDPE 5.0.2
* NTCrackPipe 2.0
* GRR 3.4.0.4
* UFONet 1.4

Kali Linux Tutorials

* 0l4bs : Cross-Site Scripting Labs For Web Application Security Enthusiasts
* CVE-API : Unofficial API for CVE.MITRE.ORG
* NekoBot : Auto Exploiter With 500+ Exploit 2000+ Shell
* Gospider : Fast Web Spider Written In Go
* DecryptTeamViewer : Enumerate & Decrypt TeamViewer Credentials From Windows Registry
* DrSemu : Malware Detection & Classification Tool Based on Dynamic Behavior
* Syborg : Recursive DNS Subdomain Enumerator With Dead-End Avoidance System
* Manul : A Coverage-Guided Parallel Fuzzer For Open-Source And Blackbox Binaries On Windows, Linux & M
* Fuzzowski : The Network Protocol Fuzzer
* Nray : Distributed Port Scanner

GBHackers Analysis

* Millions of Windows & Linux Systems are Vulnerable to Remote Hack that Manufactured by Lenovo, Dell,
* Fox Kitten - Iranian Malware Campaign Exploiting Vulnerable VPN Servers To Hack The Organizations Int
* SweynTooth - 11 Bluetooth Bugs That Affected SoC Vendors Let Hackers to Crash The Device & Execute th
* E-Scooters Can Be Hacked Using Remote Locking System Manipulation
* Adobe Released February 2020 Security Updates - Fixes Critical Bugs in 5 Software

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

* Revotech I6032B-P Remote Configuration Disclosure
* ACE SECURITY WiP-90113 HD Camera Remote Configuration Disclosure
* SecuSTATION IPCAM-130 HD Camera Remote Configuration Disclosure
* Android Binder Use-After-Free
* CandidATS 2.1.0 Cross Site Request Forgery
* DotNetNuke CMS 9.4.4 Zip Directory Traversal
* eLection 2.0 SQL Injection
* DotNetNuke CMS 9.5.0 File Extension Check Bypass
* DotNetNuke CMS 9.5.0 Cross Site Scripting
* Quick N Easy Web Server 3.3.8 Denial Of Service
* Avaya IP Office Application Server 11.0.0.0 Cross Site Scripting
* ManageEngine EventLog Analyzer 10.0 Information Disclosure
* ATutor 2.2.4 SQL Injection
* Go SSH 0.0.2 Denial Of Service
* AMSS++ 4.7 Backdoor Account
* Aptina AR0130 Camera Remote Configuration Disclosure
* SecuSTATION SC-831 HD Camera Remote Configuration Disclosure
* ESCAM QD-900 WIFI HD Camera Remote Configuration Disclosure
* Amovision AM-Q6320-WIFI HD Camera Remote Configuration Disclosure
* OpenNetAdmin Ping Command Injection
* Open-Xchange App Suite / Documents Server-Side Request Forgery
* D-Link DGS-1250 Header Injection
* Online Birth Certificate System 1.0 Cross Site Scripting
* AMSS++ 4.31 SQL Injection
* Apache James Server 2.3.2 Insecure User Creation / Arbitrary File Write

CXSecurity

* Quick N Easy Web Server 3.3.8 Denial Of Service
* Amovision AM-Q6320-WIFI HD Camera Remote Configuration Disclosure
* Revotech I6032B-P Remote Configuration Disclosure
* Aptina AR0130 Camera Remote Configuration Disclosure
* Go SSH 0.0.2 Denial Of Service
* SecuSTATION SC-831 HD Camera Remote Configuration Disclosure
* Cacti 1.2.8 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

* [local] Diamorphine Rootkit - Signal Privilege Escalation (Metasploit)
* [remote] Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)
* [local] Android Binder - Use-After-Free (Metasploit)
* [webapps] Cacti 1.2.8 - Remote Code Execution
* [webapps] Aptina AR0130 960P 1.3MP Camera - Remote Configuration Disclosure
* [webapps] DotNetNuke 9.5 - File Upload Restrictions Bypass
* [webapps] DotNetNuke 9.5 - Persistent Cross-Site Scripting
* [webapps] eLection 2.0 - 'id' SQL Injection
* [dos] Go SSH servers 0.0.2 - Denial of Service (PoC)
* [webapps] ManageEngine EventLog Analyzer 10.0 - Information Disclosure
* [webapps] I6032B-P POE 2.0MP Outdoor Camera - Remote Configuration Disclosure
* [webapps] ATutor 2.2.4 - 'id' SQL Injection
* [webapps] SecuSTATION SC-831 HD Camera - Remote Configuration Disclosure
* [webapps] AMSS++ 4.7 - Backdoor Admin Account
* [webapps] CandidATS 2.1.0 - Cross-Site Request Forgery (Add Admin)
* [dos] Quick N Easy Web Server 3.3.8 - Denial of Service (PoC)
* [webapps] SecuSTATION IPCAM-130 HD Camera - Remote Configuration Disclosure
* [webapps] AMSS++ v 4.31 - 'id' SQL Injection
* [webapps] Real Web Pentesting Tutorial Step by Step - [Persian]
* [webapps] ESCAM QD-900 WIFI HD Camera - Remote Configuration Disclosure
* [webapps] Avaya IP Office Application Server 11.0.0.0 - Reflective Cross-Site Scripting
* [dos] Core FTP Lite 1.3 - Denial of Service (PoC)
* [webapps] Easy2Pilot 7 - Cross-Site Request Forgery (Add User)
* [webapps] Nanometrics Centaur 4.3.23 - Unauthenticated Remote Memory Leak
* [webapps] DBPower C300 HD Camera - Remote Configuration Disclosure

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

* evm: ALLSTAR: New Challenge Problems for Static Analysis
* Patrick Wardle: Making the Old, New: repurposing macOS malware
* Maddie Stone: Whatsup with WhatsApp: A Detailed Walk Through of Reverse Engineering CVE-2019-3568
* Mike Bell: Extending Ghidra: from Script to Plugins and Beyond

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

* Hacking Philips Hue Lights To Hack Whole Networks - ThreatWire
* O.MG Cable, now also in USB-C and USB Micro
* Ring Android App Shares Data With Facebook - ThreatWire
* Honeypot ICS Network Tricks CyberCriminals - ThreatWire

The PC Security Channel [TPSC]

* Sophos vs Malware
* Coronavirus and Phishing
* Windows Defender vs Ransomware
* Soviet Ransomware destroys Capitalist Windows

Eli the Computer Guy

* HTML Intro - Lists
* HTML Intro - Hyperlink Navigation
* HTML Intro - Embed Images
* REVIEW - DeckLink Quad HDMI Recorder (Mac Pro and Wirecast)

Security Now

* The Internet of Troubles - Security Now 754
* Promiscuous Cookies - Security Now 753

Troy Hunt

* Weekly Update 179

Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* Cisco Releases Security Updates
* Adobe Releases Security Updates for After Effects and Media Encoder
* VMware Releases Security Updates for vRealize Operations for Horizon Adapter
* Be Cautious of Romance Scams
* North Korean Malicious Cyber Activity
* New SchoolSafety.gov Provides Cyber Guidance for K-12 Schools
* FBI Releases IC3 2019 Internet Crime Report
* AA20-049A: Ransomware Impacting Pipeline Operations
* AA20-031A: Detecting Citrix CVE-2019-19781
* AA20-020A: Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANO
* Vulnerability Summary for the Week of February 17, 2020
* Vulnerability Summary for the Week of February 10, 2020
* Vulnerability Summary for the Week of February 3, 2020

Symantec - Latest Threats

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

Symantec - Latest Risk

PUA.SafelyOnline: Type: Potentially Unwanted App.
Adware.4SharedDesktop: Type: Adware.
Hacktool.Sharpdpapi: Hacktool.Foxplace: ActiveContent.DI.1: Type: Other.
Hacktool.Sharphound: Hacktool.Safetykatz : PUA.Avrising: Type: Potentially Unwanted App.
Hacktool.ProcHack : PUA.FileConvTab: Type: Potentially Unwanted App.
PUA.Redpher: Type: Potentially Unwanted App.
Remacc.Remadmin: Type: Other.
Adware.TMAagent: Type: Adware.
Hacktool.Filensfer:

Advisories

Symantec - Latest Advisories

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

NCSC - Latest Advisories

Weekly Threat Report 14th February 2020
The NCSC's weekly threat report is drawn from recent open source reporting.
CAS(T) closed
Anne W reflects on the history of the Commodity Assurance Services (Telecommunications) scheme (CAS(T)).

Zero Day Initiative Advisories

ZDI-CAN-10325: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10321: LAquis
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10320: LAquis
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10319: LAquis
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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10316: LAquis
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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10197: LAquis
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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is

given until 2020-06-20 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-10175: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10032: Parallels

A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Reno Robert' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10031: Parallels

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 'Reno Robert' was reported to the affected vendor on: 2020-02-21, 3 days ago. The vendor is given until 2020-06-20 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-10525: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Hossein Lotfi of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10522: Microsoft

A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Hossein Lotfi of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10516: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Hossein Lotfi of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10512: Microsoft

A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Hossein Lotfi of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10318: LAquis

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10317: LAquis

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-20, 4 days ago. The vendor is given until 2020-06-19 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-10332: IBM

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

was reported to the affected vendor on: 2020-02-19, 5 days ago. The vendor is given until 2020-06-18 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-9892: 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 'Z0mb1E' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10483: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10481: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10480: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10472: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10471: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10470: Rockwell 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: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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-10459: 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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2020-02-18, 6 days ago. The vendor is given until 2020-06-17 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

Slackware Security Advisory - proftpd Updates

Slackware Security Advisory - New proftpd packages are available for Slackware 14.0, 14.1, 14.2, and -current to fix a security issue.

Red Hat Security Advisory 2020-0565-01

Red Hat Security Advisory 2020-0565-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.5.0. Memory safety issues and various other vulnerabilities have been addressed.

Red Hat Security Advisory 2020-0566-01

Red Hat Security Advisory 2020-0566-01 - The python-pillow packages contain a Python image processing library that provides extensive file format support, an efficient internal representation, and powerful image-processing capabilities. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2020-0564-01

Red Hat Security Advisory 2020-0564-01 - The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4289-1

Ubuntu Security Notice 4289-1 - Jeriko One discovered that Squid incorrectly handled memory when connected to an FTP server. A remote attacker could possibly use this issue to obtain sensitive information from Squid memory. Regis Leroy discovered that Squid incorrectly handled certain HTTP requests. A remote attacker could possibly use this issue to access server resources prohibited by earlier security filters. Guido Vranken discovered that Squid incorrectly handled certain buffer operations when acting as a reverse proxy. A remote attacker could use this issue to cause Squid to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2020-0556-01

Red Hat Security Advisory 2020-0556-01 - This release of Open Liberty 20.0.0.2 serves as a replacement for Open Liberty 20.0.0.1 and includes security fixes, bug fixes, and enhancements. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-4288-1

Ubuntu Security Notice 4288-1 - It was discovered that ppp incorrectly handled certain rhostname values. A remote attacker could use this issue to cause ppp to crash, resulting in a denial of service, or possibly execute arbitrary code.

Kernel Live Patch Security Notice LSN-0063-1

Mitchell Frank discovered that the Wi-Fi implementation in the Linux kernel when used as an access point would send IAPP location updates for stations before client authentication had completed. A physically proximate attacker could use this to cause a denial of service. It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. Various other issues were also addressed.

Red Hat Security Advisory 2020-0559-01

Red Hat Security Advisory 2020-0559-01 - KornShell is a Unix shell developed by AT&T Bell Laboratories, which is backward-compatible with the Bourne shell and includes many features of the C shell. The most recent version is KSH-93. KornShell complies with the POSIX.2 standard. A code injection vulnerability was addressed.

Red Hat Security Advisory 2020-0451-01

Red Hat Security Advisory 2020-0451-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. A TLS/SSL Birthday attack vulnerability from 2016 was addressed.

Red Hat Security Advisory 2020-0555-01

Red Hat Security Advisory 2020-0555-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM hypervisor in environments managed by Red Hat products.

Ubuntu Security Notice USN-4279-2

Ubuntu Security Notice 4279-2 - USN-4279-1 fixed vulnerabilities in PHP. The updated packages caused a regression. This update fixes the problem. It was discovered that PHP incorrectly handled certain scripts. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. It was discovered that PHP incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. It was discovered that PHP incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 19.10. Various other issues were also addressed.

Red Hat Security Advisory 2020-0553-01

Red Hat Security Advisory 2020-0553-01 - RabbitMQ is an implementation of AMQP, the emerging standard for high performance enterprise messaging. The RabbitMQ server is a robust and scalable implementation of an AMQP broker. Issues addressed include a cross site scripting vulnerability.

Debian Security Advisory 4629-1

Debian Linux Security Advisory 4629-1 - Simon Charette discovered that Django, a high-level Python web development framework, did not properly handle input in its PostgreSQL module. A remote attacker could leverage this to perform SQL injection attacks.

Ubuntu Security Notice USN-4286-2

Ubuntu Security Notice 4286-2 - USN-4286-1 fixed vulnerabilities in the Linux kernel for Ubuntu 16.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement kernel from Ubuntu 16.04 LTS for Ubuntu 14.04 ESM. It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-4287-2

Ubuntu Security Notice 4287-2 - USN-4287-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux kernel for Microsoft Azure Cloud systems for Ubuntu 14.04 ESM. It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. Various other issues were also addressed.

Citytv Video Unencrypted Analytics

The Citytv Video Android and iOS applications send potentially sensitive information such as device model and resolution, mobile carrier, days since first use, days since last use, total number of app launches, number of app launches since upgrade, and previous app session length, unencrypted to third party sites (Adobe Experience Cloud, ScorecardResearch). Citytv Video Android versions 4.08.0 and below and iOS versions 3.36 and below are affected.

Global TV Unencrypted Analytics

The Global TV Android and iOS applications send potentially sensitive information such as device model and resolution, mobile carrier, days since first use, days since last use, total number of app launches, number of app launches since upgrade, and previous app session length, unencrypted to both first (CNAME to third) and third party sites (Adobe Experience Cloud, ScorecardResearch). Global TV Android versions 2.3.2 and below and iOS versions 4.7.5 and below are affected.

Red Hat Security Advisory 2020-0550-01

Red Hat Security Advisory 2020-0550-01 - OpenJPEG is an open source library for reading and writing image files in JPEG2000 format. Issues addressed include a buffer overflow vulnerability.

Debian Security Advisory 4628-1

Debian Linux Security Advisory 4628-1 - Multiple security issues were found in PHP, a widely-used open

source general purpose scripting language which could result in information disclosure, denial of service or incorrect validation of path names.

Ubuntu Security Notice USN-4287-1

Ubuntu Security Notice 4287-1 - It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. It was discovered that the Atheros 802.11ac wireless USB device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4286-1

Ubuntu Security Notice 4286-1 - It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. It was discovered that a race condition existed in the Softmac USB Prism54 device driver in the Linux kernel. A physically proximate attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4285-1

Ubuntu Security Notice 4285-1 - It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. It was discovered that the HSA Linux kernel driver for AMD GPU devices did not properly check for errors in certain situations, leading to a NULL pointer dereference. A local attacker could possibly use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4284-1

Ubuntu Security Notice 4284-1 - It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. It was discovered that the Atheros 802.11ac wireless USB device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service. Various other issues were also addressed.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com