

POLL 1





MALWARE





MALWARE
Ransomware

A type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom is paid.

Resources

<http://www.fbi.gov/news/stories/2015/january/ransomware-irc-on-the-rise/ransomware-on-the-rise>

KEY POINTS

- A fairly new ransomware variant has been making the rounds lately
 - Computers become infected by clicking on links in malicious emails that appear to be from legitimate businesses and through compromised advertisements on popular websites
 - Directs user to a personalized victim's ransom page
- Examples
 - CryptoWall
 - CryptoWall 2.0 (its newer version)
- Mitigation
 - Recognize ransomware
 - Backup and securely store data



IDENTIFY, REPORT, AND REMOVE (IDRR) SERIES

MALWARE
QR Code Vulnerabilities

Quick Response (QR) code: a matrix barcode that can store a large amount of data, which can be processed by a reader

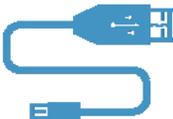
Resources
<http://money.cnn.com/2015/06/19/news/companies/ainz-kelchup-porn/>



KEY POINTS

- QR Codes have multiple functions, often transparent to the user
 - Launch websites, download files, initiate skype calls, **alter OS files and settings** and more.
 - No standard way to tell 'safe' from 'unsafe' codes
- Examples
 - Heinz Ketchup
 - Google Glass
- Mitigation
 - Only scan QR codes from trusted sources
 - Use a QR reader that lets you preview the action before launching it

CDISE CYBER AWARENESS UPDATE 2



HARDWARE

CDISE CYBER AWARENESS UPDATE

HARDWARE
Apple iPhone

Weaknesses likely introduced during code development, including specification, design, and implementation.

Resources
<https://www.us-cert.gov/hc/as/bulletins/SR15-152>

KEY POINTS

- Crafted text message causes denial of service (reboot/message disruption)
- Versions affected:
 - iOS 8.x through 8.3
- Mitigation
 - Update/patch (when available)

CDISE CYBER AWARENESS UPDATE 3

HARDWARE
Barracuda Web Filter

Man-in-the-middle attack is an attack on the authentication protocol run in which the attacker positions himself between the claimant and verifier so that he can intercept and data traveling between them.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-152>

KEY POINTS

- Uses default certificates, enabling man-in-the-middle (MITM) attacks
 - Loss of sensitive information.
 - Does not properly verify certificates.
- Vulnerable versions between 1 and 8.1.005.
- Mitigation
 - Update/Patch

CDSE CYBER AWARENESS UPDATE 4

HARDWARE
Rockwell Automation

Rockwell Software RSView 32 is a component-based human machine interface (HMI) for monitoring and controlling automation machines and processes.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-152>

KEY POINTS

- Does not properly encrypt credentials: allows local users to obtain sensitive information
- Vulnerable versions: RSView32 7.60.00 (aka CPR9 SR4) and earlier
- Mitigation
 - Update/Patch

CDSE CYBER AWARENESS UPDATE 5



SOFTWARE

CDSE CYBER AWARENESS UPDATE

SOFTWARE
Web Browsers

A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-138>

KEY POINTS

- Multiple vulnerabilities in web browsers
 - Google Chrome - Vulnerable versions before 43.0.2357.6
 - Denial of service
 - Unspecified impact
 - Execute tasks
 - Firefox - Vulnerable Versions before version 38.0
 - Allow denial of service
 - Possibly executing arbitrary code
 - May allow attacker to obtain sensitive information from memory
 - Internet Explorer - Vulnerable Versions 6-11
 - Multiple vulnerabilities allow arbitrary code or cause denial of service via crafted website
 - Mitigation: Update/Patch

CDSE CYBER AWARENESS UPDATE 6

SOFTWARE
Adobe Flash Player

Adobe Flash Player (labeled Shockwave Flash in Internet Explorer and Firefox) is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio. Flash Player can run from a web browser as a browser plug-in or on supported mobile devices

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-138>

KEY POINTS

- Multiple versions allow remote attackers to bypass protection and write to file system
- Vulnerable versions
 - Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux,
 - Adobe AIR before 17.0.0.172,
 - Adobe AIR SDK before 17.0.0.172
 - Adobe AIR SDK & Compiler before 17.0.0.172
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 7

SOFTWARE
Wireshark

Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. It is freely available as open source, and is released under the GNU General Public License version 2.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-152>

KEY POINTS

- Allow denial of service (infinite loop and CPU consumption) via crafted packet
- Vulnerable versions
 - Versions between 1.12.x and 1.12.5, 1.10.x and 1.10.14, 1.10.x-1.10.14 and 1.12.x to 1.12.5
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 8

SOFTWARE
Linux Kernel

The Linux kernel is a Unix-like computer operating system kernel. In computing, the kernel is a computer program that manages I/O (input/output) requests from software, and translates them into data processing instructions for the central processing unit and other electronic components of a computer. The kernel is a fundamental part of a modern computer's operating system.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-152>

KEY POINTS

- Allows attackers to gain privileges, denial of service, and gain write access to the file system
- Vulnerable versions
 - Kernel versions before 4.0
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 9

SOFTWARE
Cisco Unified MeetingPlace

Cisco Unified MeetingPlace is a web teleconference software which integrates audio, video, and web conferencing capabilities.

Resources
<https://www.us-cert.gov/ncas/bulletins/SB15-152>

KEY POINTS

- Allow remote attackers to inject arbitrary script, read files, or obtain sensitive information via a crafted URL or resource request
- Vulnerable versions
 - Versions 8.6(1.2) and 8.6(1.9)
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 10



HUMAN

CDSE CYBER AWARENESS UPDATE

HUMAN
 Hacktivist Targeting Law Enforcement, Military, and Government Employees

FBI Warns that law enforcement and public officials are at increasing risk of social engineering and hacking attacks

Resources
<http://www.ic3.gov/media/2015/150421.aspx>

KEY POINTS

- Hacktivism: The often-subversive use of computers and computer networks to promote a political agenda.
- FBI warns of activity against government personnel
 - Doxing
 - Swatting
 - Cyber attacks
- Mitigation
 - Privacy settings/OPSEC on Social Networking Sites
 - Security on home computers/wireless
 - Phishing awareness
 - Social engineering awareness
 - Monitor web and credit reports
 - Two-factor authentication on email

June 2015

CDSE CYBER AWARENESS UPDATE 11

NETWORK



CDSE CYBER AWARENESS UPDATE

NETWORK
 Cisco

A network is information systems implemented with a collection of interconnect components. Such components may include routers, hubs, cabling, telecommunication, controllers, key distribution centers and technical control devices.

Resources
http://www.wisc.edu/cybersecurity/cybersecurity/0815_116

KEY POINTS

- Multiple vulnerabilities in multiple products
 - Access server, web security system, wireless systems, etc. Allows remote attacks, sessions hijacks, file uploads, script injection, denial of service, and other attacks.
- Vulnerable versions
 - Cisco Unified Communications Manager 10.0
 - Cisco Wireless LAN Controller (WLC) devices before 7.0.241, 7.1.x through 7.4.x before 7.4.122, and 7.5.x and 7.6.x before 7.6.120
 - Cisco Secure Access Control Server Solution Engine (ACSE) 5.5(0.1)
 - Cisco IOS 15.3S
 - Cisco Unified Intelligence Center 10.6(1)
 - Cisco FireSIGHT System Software 5.3.0
 - Multiple others
- Do you know hardware configuration? Does it impact you?
- Mitigation: Update

June 2015

CDSE CYBER AWARENESS UPDATE 12

NETWORK
Bluecoat web appliance

Firmware is computer programs and data stored in hardware - typically in read-only-memory (ROM) - such that the program and data can not be dynamically be rewritten or modified during execution of the program

Resources
<https://www.us-cert.gov/hcra/bulletins/SB15-159>

KEY POINTS

- May allow attackers to hijack web sessions and administrator authentications
- Vulnerable versions
 - Versions 3.6.x and 3.8.x before 3.8.4
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 13

NETWORK
Aruba Networks ClearPass Policy Manager

The Aruba ClearPass Policy Manager™ platform provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure.

Resources
<https://www.us-cert.gov/hcra/bulletins/SB15-152>

KEY POINTS

- May allow attackers to hijack web sessions and administrator authentications
- Vulnerable versions: Before 6.5.0
- Mitigation
 - Update/patch

CDSE CYBER AWARENESS UPDATE 14

“WHAT DO I NEED TO DO?”
Recommendations

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”
- Bruce Schneier

Resources
CDSE: <http://www.cdse.edu>
US CERT Bulletins: <https://www.us-cert.gov/hcra>
Internet Crime Complaint Center: <http://www.ic3.gov/default.aspx>

WHAT IS MY ROLE IN THIS?

1. Form a relationship/partnership with your IT and cybersecurity departments
2. Know what's on your network (hardware and software)
3. Review/sign up for alerts through US CERT
4. Use CDSE resources, such as webinars, free eLearning courses, and more

CDSE CYBER AWARENESS UPDATE 15

POLL 2



CDSE  CYBER AWARENESS UPDATE



QUESTIONS?

CDSE  CYBER AWARENESS UPDATE



THANKS FOR JOINING US!
CHECK OUT OUR UPCOMING WEBINARS:

- Privileged User webinar: July 9, 2015
- RMF Steps 1-6 Courses: July 2015
- Update to CDSE Virtual Environments
 - o Current VE is being broken out into three unique environments for ease of use
 - o Updated student workbooks
 - o Upgraded Red Hat Enterprise Linux 6 environment

CDSE  CYBER AWARENESS UPDATE
