INFORMATION WARFARE CENTER V3.0

CYBER INTELLIGENCE REPORT

MARCH 25, 2015

The IWC CIR is an OSINT resource focusing on advanced persistent threats and other digital dangers. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage.

SUMMARY

Symantec ThreatCon Level 2 - Medium: Increased alertness

This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating.

WEEK IN REVIEW

Several legal issues are in the public eye, including Net Neutrality, CISA, making spying on citizens easier, and allowing the Department of Justice the ability to hack your computers. The landscape is changing. The question is, is it changing for better or for worse.

Here are some items of interest (links below):

- NYPD Officer Arrested For Hacking FBI Databases.
- New York County Sheriff Must Give Up Stingray Records.
- Facebook PRISM Data Case Heads To European High Court.

PROMOTIONS

Military, Law Enforcement, and Emergency Services receive 10% off cyber security training from the Information Warfare Center. This sale is good through 2015 for courses ranging from the Certified Ethical Hacker, Computer Forensics, to the CISSP. If you would like more information, contact sales@informationwarfarecenter.com and mention the sale "online thirds". Attached is a link to the flyer.

NEWS: INFORMATION WARFARE

- US accusations of Israeli espionage – why now? - Ynetnews.
- The Precise (and Narrow) Limits On US Economic Espionage - Lawfare (blog).
- Corporate espionage: CBI has hours of call records of top officials, say sources - Econoı
- Don't get caught: golden rule for espionage among friends - The Times (subscription).
- Why one of the world's leading cyber-espionage firms won't touch Russia - SFGate.
- 'Threat-sharing' cybersecurity bill introduced in US House - Reuters.
- ISIS sends Cyber threat to U.S. military members - FOX 29.
- UK Report Highlights Role of Insurance in Managing, Mitigating Cyber Risk - Insurance Journal.
- Airbus awarded £1.4m to build 3D virtual reality cyber centre for MoD - V3.co.uk.
- A quarter of users don't understand the risks of Mobile Cyberthreats - IT News Africa.
- Wind Turbine Blown Away By Control System Vulnerability.
- Google And Mozilla Block Bogus Certificates From China.
- Facebook PRISM Data Case Heads To European High Court.
- Net Neutrality Legal Challenge Launched.
- Small Biz Cisco Phones Open To Eavesdrop 0-Day.
- UK Lack Of Cyber Insurance Exposed.
- Stealing Data From Computers Using Heat.
- PoSeidon, Brother Of Zeus, Forks Up Point Of Sale Terminals.
- Drupal SQL Injection Vulnerabilities Persist, Despite Patch.
- All Four Major Browsers Take A Stomping At Pwn2Own Hacking Contest.
- Amended CISA Bill Can Still Further Govt Surveillance.
- MRIs Show Our Brains Shutting Down When We See Security Prompts.
- How To Tell Which Of Your Emails Are Being Tracked.
- US Threatened Berlin With Intel Blackout Over Snowden Asylum.
- New BIOS Implant, Vulnerability Discovery Tool To Debut At CanSecWest.
- NYPD Officer Arrested For Hacking FBI Databases.
- Operation Woolen Goldfish Hackers Spear Phishing European Firms.
- Pinterest Throws Cash At Topless Bug Finders.
- Target Pitches $10m Settlement Following Mega Data Breach.
- Mysterious 'High Priority' OpenSSL Security Fix Incoming.
- Report: Committee Approves Rule Change That Expands FBI's Hacking Authority.
- New York County Sheriff Must Give Up Stingray Records.
- Fatally Flawed RC4 Should Just Die, Shout Angry Securobods.
- National Archives Crowdsources Transcription Of CIA Files.
- U.S. Senator Introduces Bill Aimed At Federal Breach Notification Standard.

NEWS: HIPPA

- Premera breach: Are HIPAA standards too low? - Help Net Security.
- Top Tips on Conducting a HIPAA Risk Assessment - HealthITSecurity.com.
- HIPAA crackdown extends beyond health care providers - The Tennessean.
- EHR Compliance And HIPAA Compliance: Help Your Healthcare IT Clients ...
- What Are the Legal Concerns in a HIPAA Risk Assessment? - HealthITSecurity.com.

NEWS: SCADA

- Global Compressor Control System (Controlling Component (PLC and SCADA ... - PR News.
- DAQ/Visualization Software collects data from diverse sources. - ThomasNet News.
- How 'Power fingerprint' could improve security for ICS/SCADA systems - CSO Online.
- BRS Labs Launches Artificial-Intelligence-Based SCADA Analysis Portal - Yahoo Finance UK.
- CeBIT Innovation: gateprotect Offers Unique New SCADA Protection for Energy ... - Virtual-Strategy Magazine (press release)

NEWS: CYBER LAWS & LEGISLATION

- Senate Intelligence Committee Advances Terrible ... - EFF.
- 'Threat-sharing' cybersecurity bill introduced in US House - Reuters.
- It's time to update antiquated cybersecurity legislation - Washington Examiner.
- Legislation Would Criminalize Revenge Porn; Allow Search Warrants for Cyber ... - SCVNEWS.com.
- Battle Over Cyber Bill Reveals Fissure Between States and DC - American Banker.

NEWS: COMPUTER FORENSICS

- Companies turn to forensic investigators to detect cyber crime - Channel News Asia.
- I'm a feminist, and I'm glad the Senate sex trafficking bill stalled - The Week Magazine.
- Karnataka Police commissions fully equipped cyber forensic lab - The Indian Express.
- Man accused of video voyeurism in golf course restroom - Tampabay.com (blog).
- Seven face charges after Friday raid in Thibodaux - Daily Comet.

EXPLOITS

- Wordpress InfusionSoft Shell Upload.
- WordPress OptimizePress Theme Shell Upload.
- WordPress cache_lastpostdate Arbitrary Code Execution.
- WordPress W3 Total Cache PHP Code Execution.
- WordPress Foxypress uploadify.php Arbitrary Code Execution.
- Anchor CMS 0.9.2 Cross Site Scripting.
- Joomla Random Article SQL Injection.
- Unasjee CMS Cross Site Request Forgery.
- Manage Engine Device Expert 5.9.9.0 Cross Site Scripting.
- Powershell Remoting Remote Command Execution.
- Exim GHOST (glibc gethostbyname) Buffer Overflow.
- Belkin Play N750 login.cgi Buffer Overflow.
- Firefox Proxy Prototype Privileged Javascript Injection.
- Cisco UCSM 2.2 Username / Password Disclosure.
- openEMR 4.2.0 Cross Site Scripting / SQL Injection.
- DokuWiki 2014-09-29c Cross Site Scripting.
- ManageEngine Network Configuration Management CSRF.
- WordPress InBoundio Marketing Shell Upload.
- WordPress MP3-Jplayer 2.1 Local File Disclosure.
- Manage Engine Device Expert 5.9.9.0 Cross Site Scripting.
- WordPress AB Google Map Travel CSRF / XSS.
- Manage Engine Device Expert 5.9.9.0 CSRF.
- Joomla Spider FAQ SQL Injection.
- Free MP3 CD Ripper Buffer Overflow.
- WordPress Ajax Search Pro Remote Code Execution.
- WordPress Plugin InBoundio Marketing 1.0 - Shell Upload Vulnerability.
- Bsplayer 2.68 - HTTP Response Exploit (Universal).
- Wordpress Marketplace 2.4.0 - Arbitrary File Download.
- Free MP3 CD Ripper 2.6 - Local Buffer Overflow.
- Joomla Spider FAQ Component - SQL Injection Vulnerability.
- Telescope <= 0.9.2 - Markdown Persistent XSS.
- Firefox Proxy Prototype Privileged Javascript Injection.
- Citrix NITRO SDK - Command Injection Vulnerability.
- Citrix Command Center - Credential Disclosure.

CVE ADVISORIES

- CVE-2015-2680.
  - 2015-03-23
    Cross-site request forgery (CSRF) vulnerability in MetalGenix GeniXCMS before 0.0.2 allows remote attackers to hijack the authentication of administrators for requests that add an administrator account via a request in the users page to gxadmin/index.php. (CVSS:0.0) (Last Update:2015-03-23)
- CVE-2015-2679.
  - 2015-03-23
    Multiple SQL injection vulnerabilities in MetalGenix GeniXCMS before 0.0.2 allow remote attackers to execute arbitrary SQL commands via the (1) page parameter to index.php or (2) username parameter to gxadmin/login.php. (CVSS:0.0) (Last Update:2015-03-23)
- CVE-2015-2678.
  - 2015-03-23
    Multiple cross-site scripting (XSS) vulnerabilities in MetalGenix GeniXCMS before 0.0.2 allow remote attackers to inject arbitrary web script or HTML via the (1) cat parameter in the categories page to gxadmin/index.php or (2) page parameter to index.php. (CVSS:0.0) (Last Update:2015-03-23)
- CVE-2015-2564.
  - 2015-03-20
    SQL injection vulnerability in client-edit.php in ProjectSend (formerly cFTP) r561 allows remote authenticated users to execute arbitrary SQL commands via the id parameter to users-edit.php. (CVSS:6.5) (Last Update:2015-03-23)

ADVISORIES

- HP Security Bulletin HPSBST03196 1.
  - Tue, 24 Mar 2015 17:08:23 GMT
    HP Security Bulletin HPSBST03196 1 - A potential security vulnerability has been identified with HP StoreEver MSL6480 Tape Library running Bash. This is the Bash Shell vulnerability known as "Shellshock" which could be exploited remotely to allow execution of code. Revision 1 of this advisory.
- Ubuntu Security Notice USN-2545-1.
  - Tue, 24 Mar 2015 17:08:14 GMT
    A flaw was discovered in the automatic loading of modules in the crypto subsystem of the Linux kernel. A local user could exploit this flaw to load installed kernel modules, increasing the attack surface and potentially using this to gain administrative privileges.
- Ubuntu Security Notice USN-2546-1.
  - Tue, 24 Mar 2015 17:08:04 GMT
    Ubuntu Security Notice 2546-1 - A flaw was discovered in the automatic loading of modules in the crypto subsystem of the Linux kernel. A local user could exploit this flaw to load installed kernel modules, increasing the attack surface and potentially using this to gain administrative privileges. A flaw was discovered in the crypto subsystem when screening module names for automatic module loading if the name contained a valid crypto module name, eg. vfat(aes).

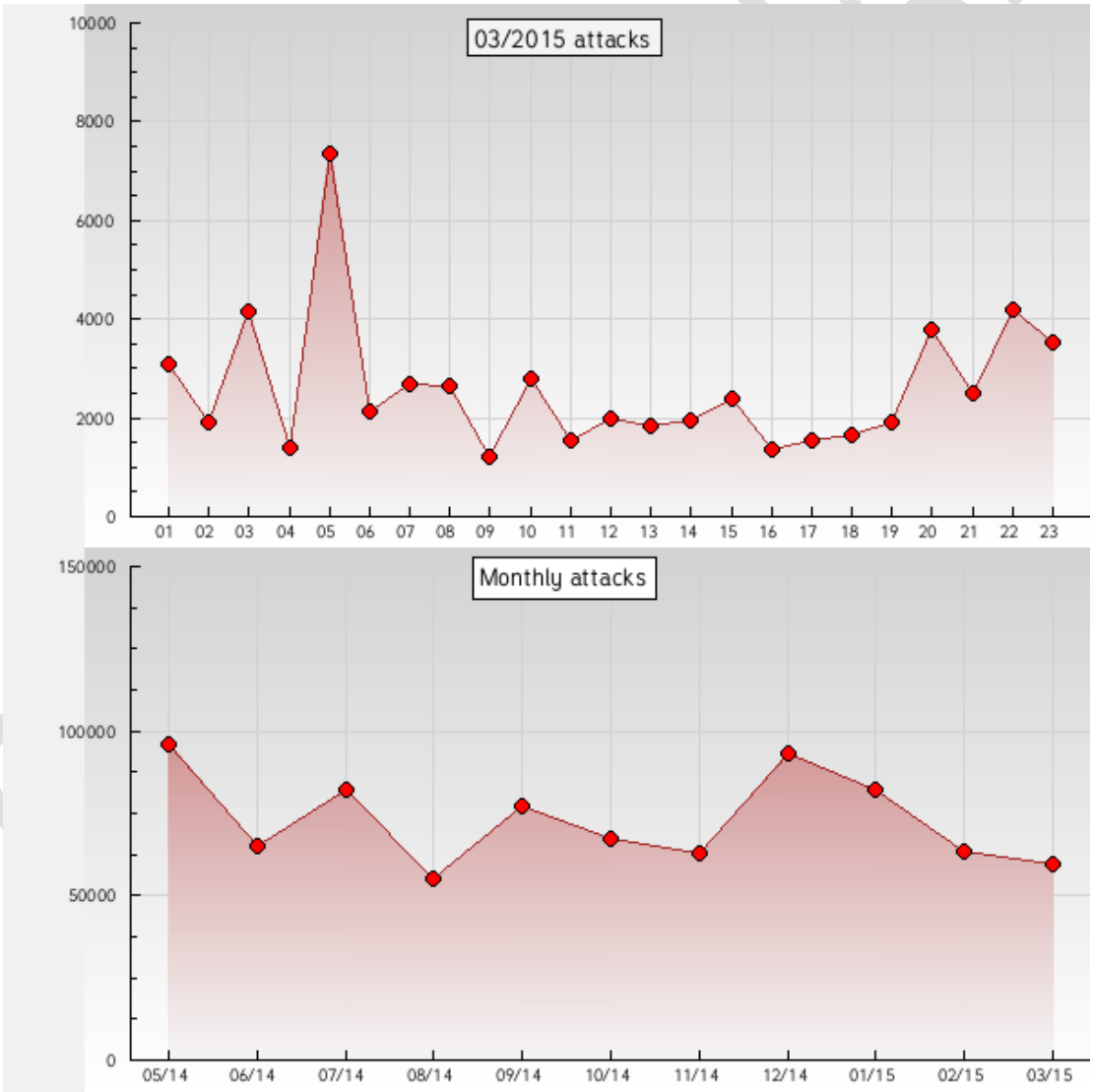
- Ubuntu Security Notice USN-2541-1.
  - Tue, 24 Mar 2015 17:07:57 GMT
    Ubuntu Security Notice 2541-1 - The Linux kernel's splice system call did not correctly validate its parameters. A local, unprivileged user could exploit this flaw to cause a denial of service (system crash). A flaw was discovered in how Thread Local Storage (TLS) is handled by the task switching function in the Linux kernel for x86_64 based machines. A local user could exploit this flaw to bypass the Address Space Layout Randomization (ASLR) protection mechanism. Various other issues were also addressed.
- Ubuntu Security Notice USN-2544-1.
  - Tue, 24 Mar 2015 17:07:48 GMT
    Ubuntu Security Notice 2544-1 - Eric Windisch discovered flaw in how the Linux kernel's XFS file system replaces remote attributes. A local access with access to an XFS file system could exploit this flaw to escalate their privileges. A flaw was discovered in the automatic loading of modules in the crypto subsystem of the Linux kernel. A local user could exploit this flaw to load installed kernel modules, increasing the attack surface and potentially using this to gain administrative privileges. Various other issues were also addressed.
- Ubuntu Security Notice USN-2543-1.
  - Tue, 24 Mar 2015 17:07:35 GMT
    Ubuntu Security Notice 2543-1 - Eric Windisch discovered flaw in how the Linux kernel's XFS file system replaces remote attributes. A local access with access to an XFS file system could exploit this flaw to escalate their privileges. A flaw was discovered in the automatic loading of modules in the crypto subsystem of the Linux kernel. A local user could exploit this flaw to load installed kernel modules, increasing the attack surface and potentially using this to gain administrative privileges. Various other issues were also addressed.
- Ubuntu Security Notice USN-2542-1.
  - Tue, 24 Mar 2015 17:07:28 GMT
    Ubuntu Security Notice 2542-1 - The Linux kernel's splice system call did not correctly validate its parameters. A local, unprivileged user could exploit this flaw to cause a denial of service (system crash). A flaw was discovered in how Thread Local Storage (TLS) is handled by the task switching function in the Linux kernel for x86_64 based machines. A local user could exploit this flaw to bypass the Address Space Layout Randomization (ASLR) protection mechanism. Various other issues were also addressed.
- Red Hat Security Advisory 2015-0716-01.
  - Tue, 24 Mar 2015 17:07:18 GMT
    Red Hat Security Advisory 2015-0716-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength, general purpose cryptography library. An invalid pointer use flaw was found in OpenSSL's ASN1_TYPE_cmp() function. A remote attacker could crash a TLS/SSL client or server using OpenSSL via a specially crafted X.509 certificate when the attacker-supplied certificate was verified by the application. An integer underflow flaw, leading to a buffer overflow, was found in the way OpenSSL decoded malformed Base64-encoded inputs. An attacker able to make an application using OpenSSL decode a specially crafted Base64-encoded input could use this flaw to cause the application to crash. Note: this flaw is not exploitable via the TLS/SSL protocol because the data being transferred is not Base64-encoded.
- HP Security Bulletin HPSBGN03249 2.

- Tue, 24 Mar 2015 17:07:11 GMT
  HP Security Bulletin HPSBGN03249 2 - Potential security vulnerabilities has been identified with HP ArcSight Enterprise Security Manager (ESM) and HP ArcSight Logger. These vulnerabilities could be exploited remotely resulting in multiple vulnerabilities. Revision 2 of this advisory.

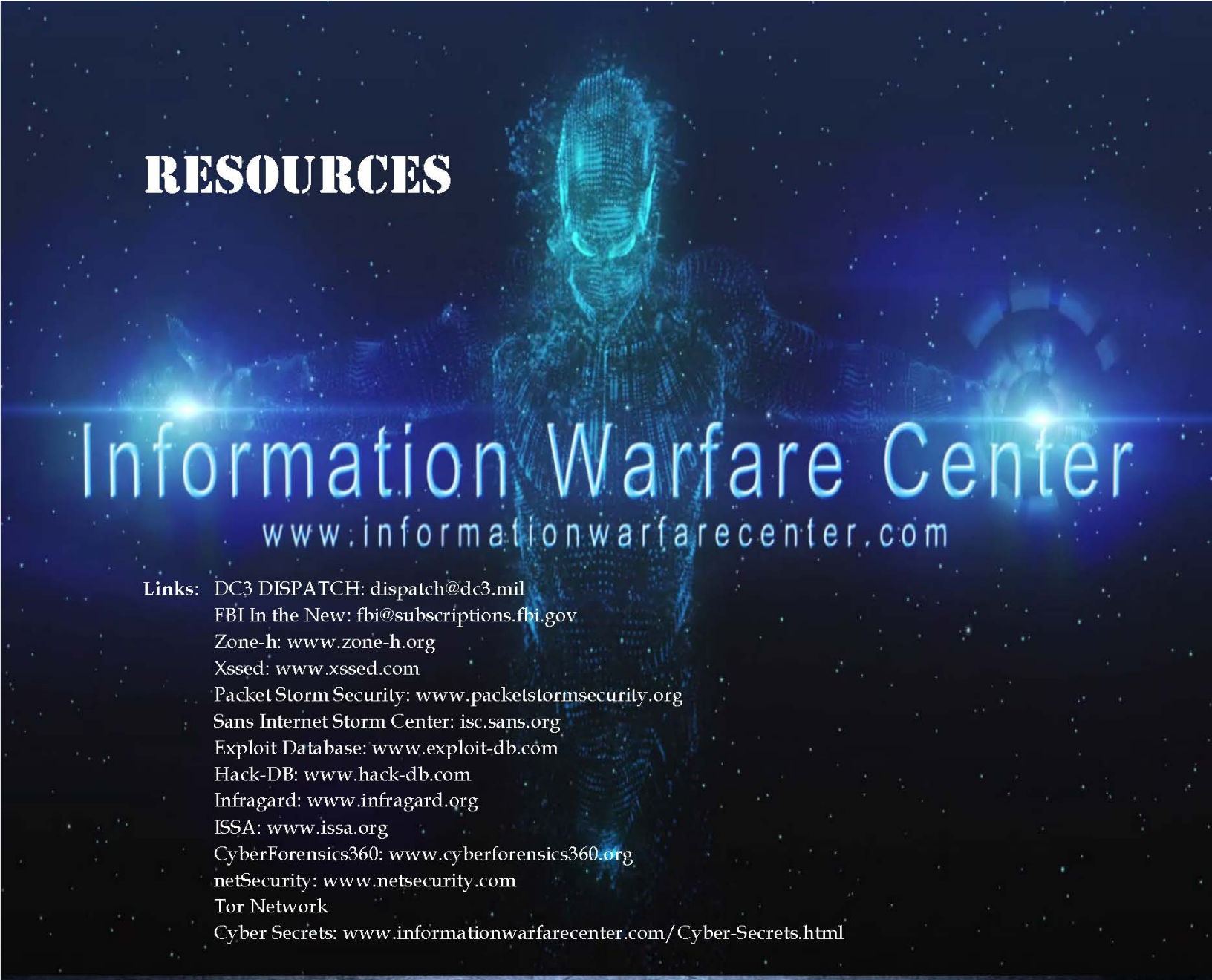
- HP Security Bulletin HPSBMU03220 1.
  - Tue, 24 Mar 2015 17:07:02 GMT
    HP Security Bulletin HPSBMU03220 1 - Potential security vulnerabilities have been identified with HP Shunra Network Appliance / HP Shunra Wildcat Appliance running Bash Shell. The vulnerabilities, known as "Shellshock", could be exploited remotely to allow execution of code. Revision 1 of this advisory.
- HP Security Bulletin HPSBHF03289 1.
  - Tue, 24 Mar 2015 17:05:09 GMT
    HP Security Bulletin HPSBHF03289 1 - A potential security vulnerability has been identified with HP ThinPro Linux This is the glibc vulnerability known as "GHOST", which could be exploited remotely to allow execution of arbitrary code. This update also addresses other vulnerabilities in SSL that would remotely allow denial of service, disclosure of information and other vulnerabilities. Revision 1 of this advisory.
- HP Security Bulletin HPSBHF03279 2.
  - Tue, 24 Mar 2015 17:03:44 GMT
    HP Security Bulletin HPSBHF03279 2 - Potential security vulnerabilities have been identified with certain HP Point of Sale PCs Running Windows with OLE Point of Sale (OPOS) Drivers. These vulnerabilities could be remotely exploited resulting in execution of code. Revision 2 of this advisory.
- HP Security Bulletin HPSBGN03299 1.
  - Tue, 24 Mar 2015 17:03:36 GMT
    HP Security Bulletin HPSBGN03299 1 - Potential security vulnerabilities have been identified with HP IceWall SSO Dfw, SSO Certd, MCRP, and Federation Agent running OpenSSL including: The SSL vulnerability known as "FREAK", which could be exploited remotely to allow disclosure of information. Other vulnerabilities which could be exploited remotely resulting in unauthorized access. Revision 1 of this advisory.
- Ubuntu Security Notice USN-2547-1.
  - Tue, 24 Mar 2015 17:03:29 GMT
    Ubuntu Security Notice 2547-1 - It was discovered that the Mono TLS implementation was vulnerable to the SKIP-TLS vulnerability. A remote attacker could possibly use this issue to perform client impersonation attacks. It was discovered that the Mono TLS implementation was vulnerable to the FREAK vulnerability.

ZONE-H ATTACK STATISTICS:

N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	Barbaros-DZ	3449	157	3606	1223	2383
2.	Ashiyane Digital Security Team	2868	4112	6980	1318	5662
3.	Hmei7	2850	1511	4361	775	3586
4.	LatinHackTeam	1438	1266	2704	2254	450
5.	iskorpitx	1324	955	2279	786	1493
6.	Fatal Error	1113	1725	2838	2458	380
7.	HighTech	945	3748	4693	3760	933
8.	chinahacker	889	1344	2233	4	2229
9.	MCA-CRB	854	626	1480	374	1106
10.	By_aGReSiF	758	1428	2186	802	1384



RESOURCES



Links: DC3 DISPATCH: dispatch@dc3.mil
FBI In the New: fbi@subscriptions.fbi.gov
Zone-h: www.zone-h.org
Xssed: www.xssed.com
Packet Storm Security: www.packetstormsecurity.org
Sans Internet Storm Center: isc.sans.org
Exploit Database: www.exploit-db.com
Hack-DB: www.hack-db.com
Infragard: www.infragard.org
ISSA: www.issa.org
CyberForensics360: www.cyberforensics360.org
netSecurity: www.netsecurity.com
Tor Network
Cyber Secrets: www.informationwarfarecenter.com/Cyber-Secrets.html