Are You Prepared for More High-Impact Vulnerabilities?

Risk Mitigation & Incident Response Strategies for the Next Heartbleed or Shellshock

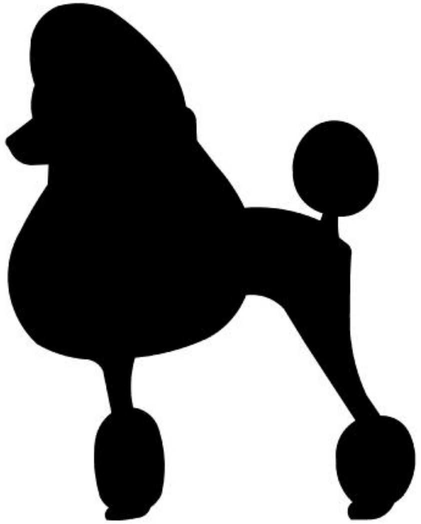
Travis Smith
Senior Security Research Engineer
Tripwire Inc.
tsmith@tripwire.com

What Is A **High Impact Vulnerability**?

A vulnerability that has both a wide distribution and high risk of exploitation.

Heartbleed
CVE-2014-0160

Shellshock/Bugbash
CVE-2014-6271



POODLE
CVE-2014-3566

Heartbleed

OpenSSL Vulnerability

- Active exploit released almost immediately … test itself was an exploit
- Harvest data in RAM – credentials, keys, data
- Affected 2/3 of Internet connected systems
- **No trace** until IDS signature was provided
- Window of time systems exposed

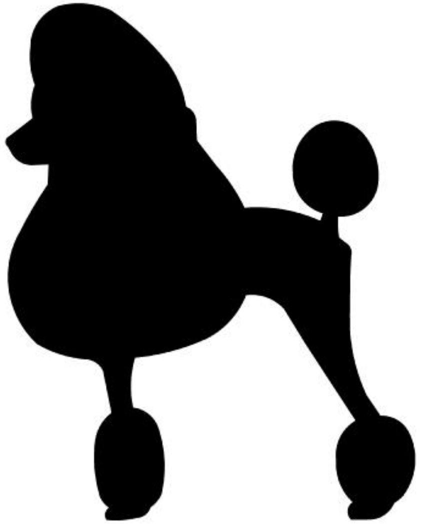
Shellshock/Bashbug

Bash Vulnerability

- Vulnerability in Bash, allowing remote code execution
- Exploit available nearly immediately
- Remote exploit with reverse shell etc
- **Evidence of exploit in logs**

POODLE

Another OpenSSL Vulnerability - Padding Oracle On Downgraded Legacy Encryption



- Widespread but difficult/unlikely exploit
  - Requires attacker to be on on the same network
  - Requires Javascript
- Attack is focused primarily on clients, MITM style attack vs remote server exploit
- Still a risk, but less enterprise risk than other major exploits

Marketing vs Actual Risk

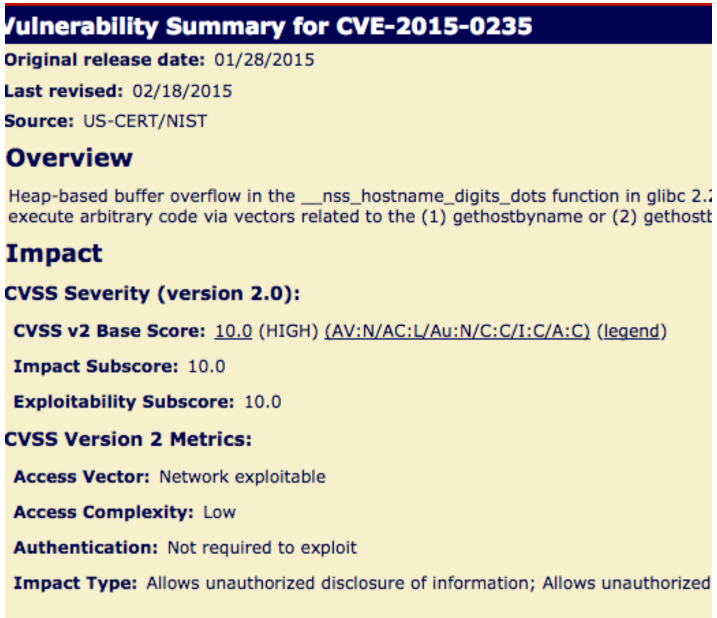
THE FUD FACTOR

- Several “high impact” vulnerabilities have been touted in the media that actually pose little no risk to the enterprise
- Security researchers are branding vulnerabilities they discover for media exposure
- Not all high impact vulnerabilities are equal

CVSS Version 2 Scoring

Does this one go to 11?

CHOST
CVE 2015-0235
CVSS Score 10:



/ulnerability Summary for CVE-2015-0235

Original release date: 01/28/2015

Last revised: 02/18/2015

Source: US-CERT/NIST

Overview

Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2 execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostb

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

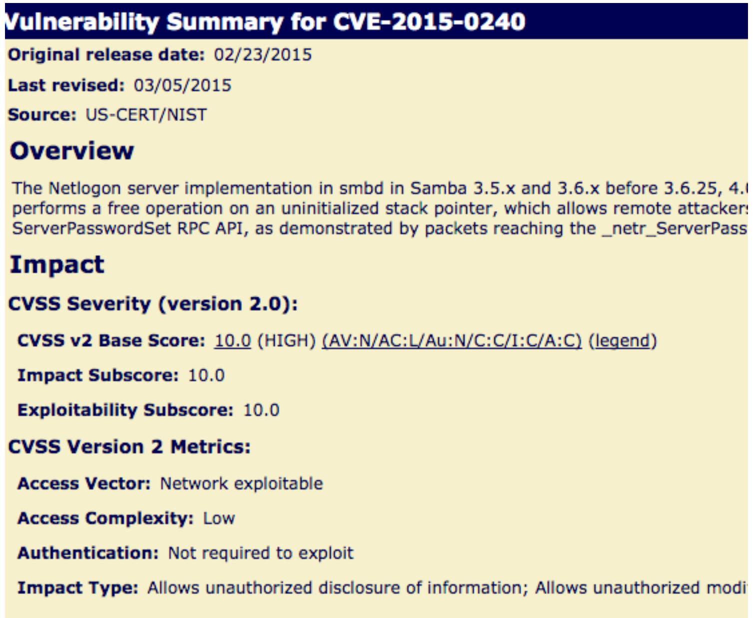
Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized

Samba Remote Code Execution
CVE-2015-0240
CVSS Score 10:



/ulnerability Summary for CVE-2015-0240

Original release date: 02/23/2015

Last revised: 03/05/2015

Source: US-CERT/NIST

Overview

The Netlogon server implementation in smbd in Samba 3.5.x and 3.6.x before 3.6.25, 4.(performs a free operation on an uninitialized stack pointer, which allows remote attacker: ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPass

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

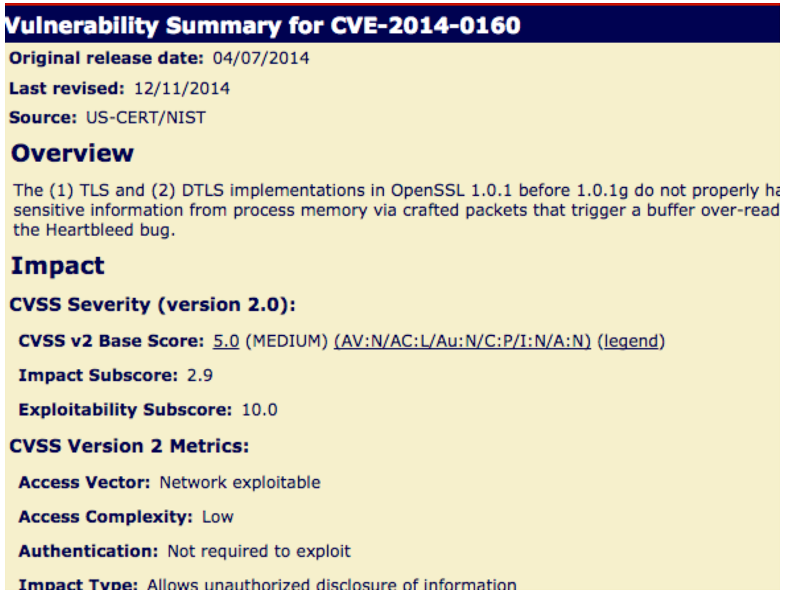
Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modi

Heartbleed
CVE-2014-0160
CVSS Score 5?



Vulnerability Summary for CVE-2014-0160

Original release date: 04/07/2014

Last revised: 12/11/2014

Source: US-CERT/NIST

Overview

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly ha sensitive information from process memory via crafted packets that trigger a buffer over-read the Heartbleed bug.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

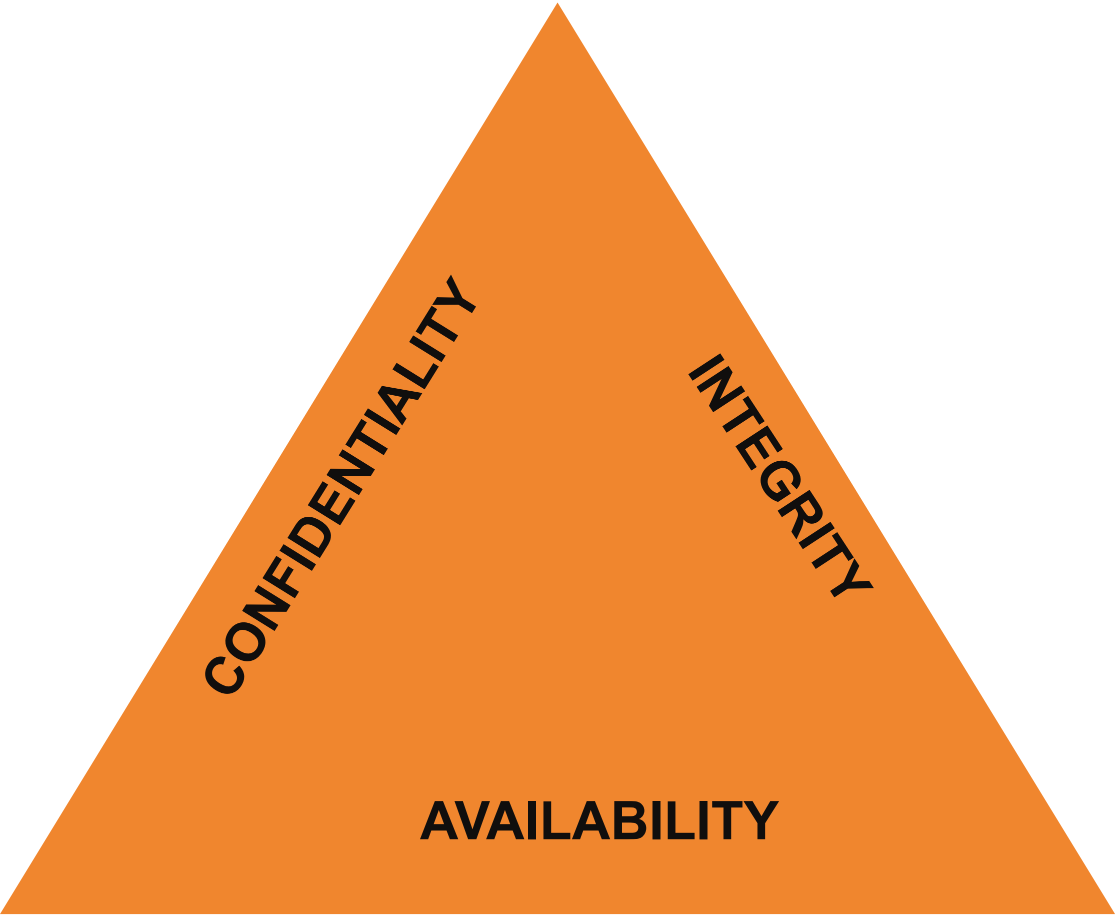
Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information

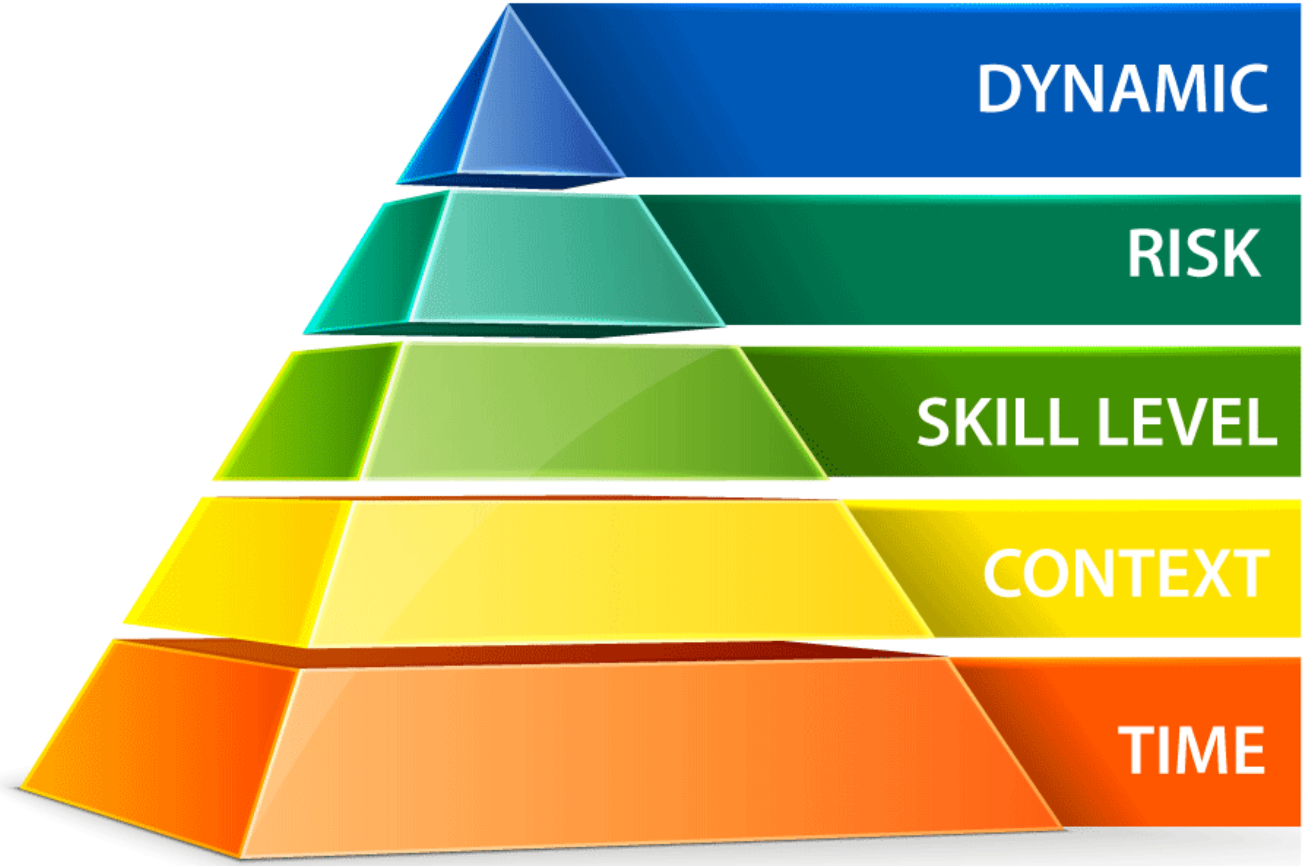
Not All Scoring Is Equal

CVSS v2



1-10

VERT VULERNABILITY SCORING



0-60,000

Tripwire VERT

TRIPWIRE®

VERT

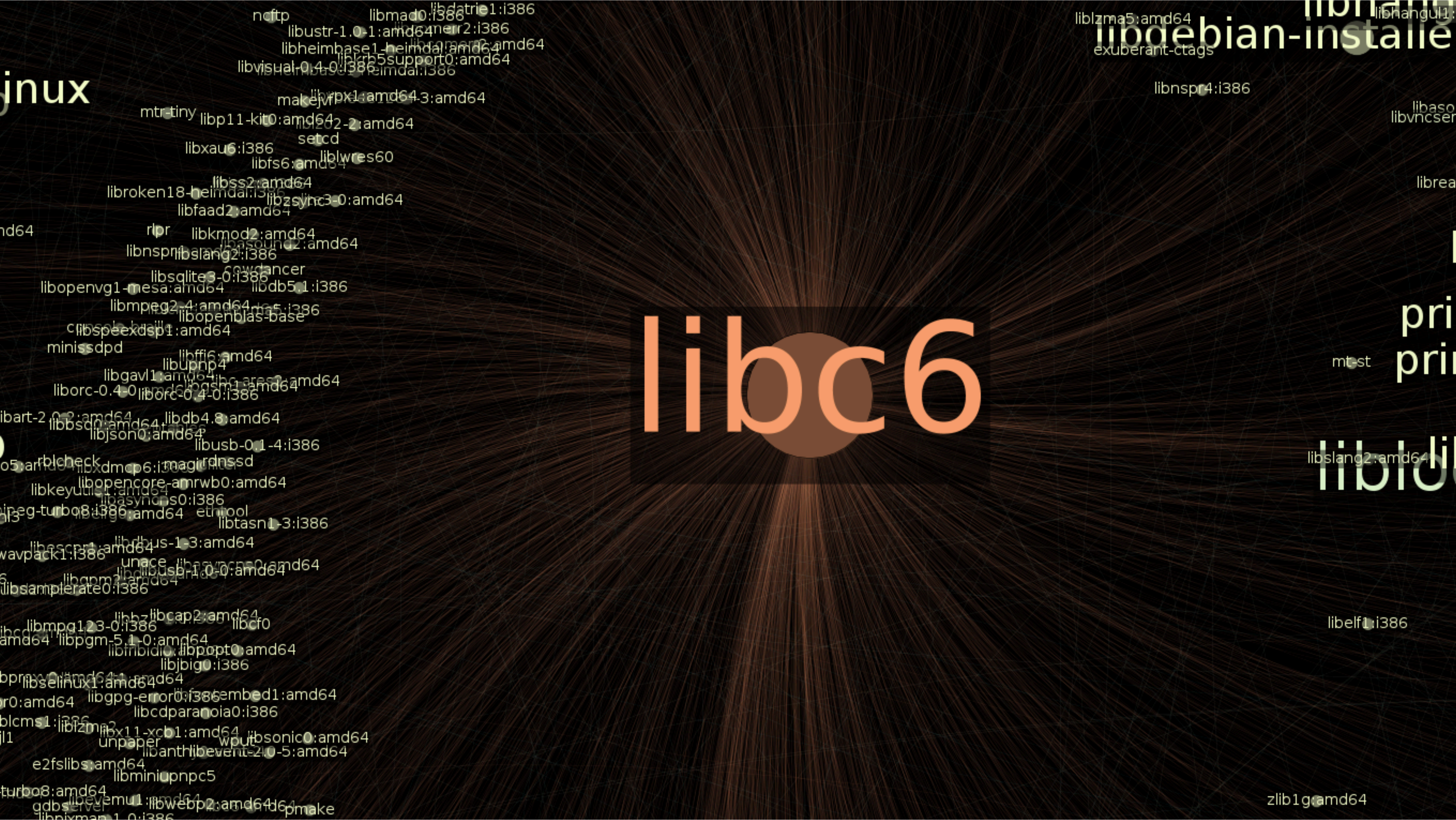
tripwire.com/vert

Forecast Calls for More High Impact Vulnerabilties

Mo Money Mo Problems

- More researchers + higher pay
- Security is a top target (SSL, encryption, tools)
- Libraries under attack
- Embedded flaws difficult/impossible to update

IN A LINUX DISTRIBUTION NOT SO FAR AWAY


libc6
ncftp
libmad0:i386
libdatrie1:i386
libustr-1.0-1:amd64
libheimbase1-heimdal:amd64
libkrb5support0:amd64
libvisual-0.4-0:i386
libheimbase1-heimdal:i386
makejvf
libvpx1:amd64
mtr-tiny
libp11-kit0:amd64
setcd
libxau6:i386
liblwres60
libfs6:amd64
libss2:amd64
libroken18-heimdal:i386
libzsync
libfaad2:amd64
rlpr
libkmod2:amd64
libasound2:amd64
libslang2:i386
cowdancer
libsqlite3-0:i386
libopenvg1-mesa:amd64
libdb5.1:i386
libmpeg2-4:amd64
libopenblas-base
libspeexdsp1:amd64
minissdpd
libffi6:amd64
libupnp4
libgavl1:amd64
liborc-0.4-0:amd64
libgsm1:amd64
liborc-0.4-0:i386
libdb4.8:amd64
libbsd0:amd64
libjson0:amd64
libusb-0.1-4:i386
rblcheck
rdnssd
libxdmcp6:i386
libopencore-amrwb0:amd64
libkeyutils1:amd64
libasyncns0:i386
ethtool
libtasn1-3:i386
libdbus-1-3:amd64
wavpack1:i386
unace
libusb-1.0-0:amd64
libsamplerate0:i386
libcap2:amd64
libcf0
libmpg123-0:i386
libpgm-5.1-0:amd64
libpopt0:amd64
libjbig0:i386
libselinux1:amd64
libgpg-error0:i386
libfreembed1:amd64
libcdparanoia0:i386
libx11-xcb1:amd64
unpaper
wput
libsonic0:amd64
libevent-2.0-5:amd64
e2fslibs:amd64
libminiupnpc5
libwebp2:amd64
pmake
liblzma5:amd64
libdebian-installer
exuberant-ctags
libnspr4:i386
mt-st
libslang2:amd64
libelf1:i386
zlib1g:amd64
jnux

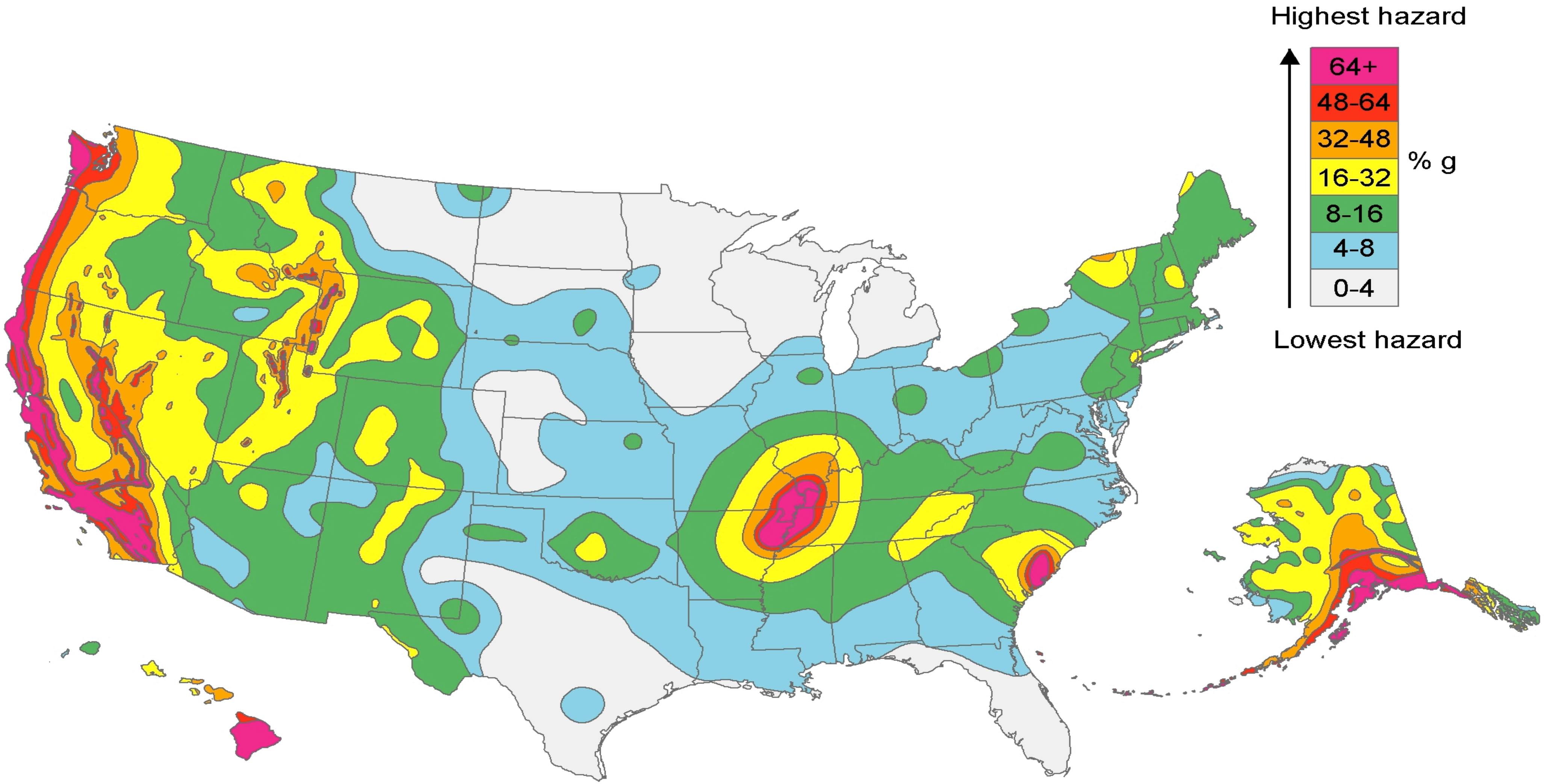
HIGH IMPACT VULNERABILITY RISK MANAGEMENT

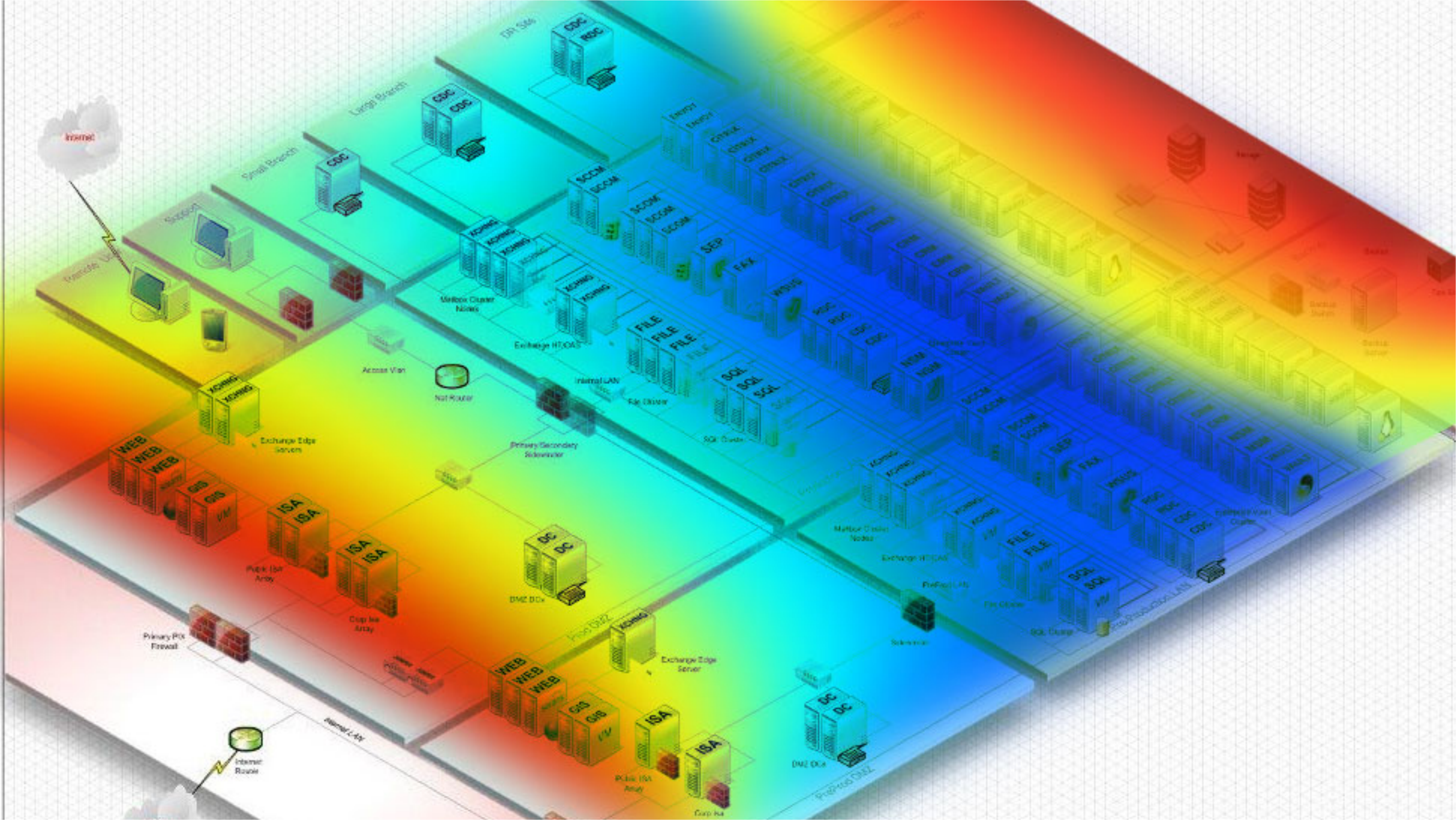
U.S. Department of Homeland Security

FEMA

RISK = HAZARD + EXPOSURE + VULNERABILITY

Earthquakes & Exploits




Internet
Remote Users
Support
Small Branch
Large Branch
DR Site
CDC
RDC
SCCM
SCOM
XCHNG
CITRIX
SEP
FAX
WSUS
FILE
SQL
VM
Mailbox Cluster Nodes
Exchange HT/CAS
Access Vlan
Nat Router
Internal LAN
File Cluster
SQL Cluster
Primary/Secondary Sidewinder
Exchange Edge Servers
WEB
GIS
ISA
Public ISA Array
Corp Isa Array
DC
DMZ DCs
Primary PIX Firewall
Prod DMZ
Internet Router
Exchange Edge Server
PreProd LAN
Sidewinder
PreProd DMZ
Storage
Backup
Backup Server

Tripwire IP360 Vulnerability Scoring

Automated Exploit	46	7	12	14	32	46	42
Easy	32	3	13	10	19	34	23
Moderate	6	4	0	4	10	12	13
Difficult	25	26	19	36	71	130	54
Extremely Difficult	8	29	16	60	28	39	53
No Known Exploit	92	41	60	140	90	153	285
	Exposure	Local Availability	Local Access	Remote Availability	Remote Access	Local Privileged	Remote Privileged

Reduce Risk – Take Inventory

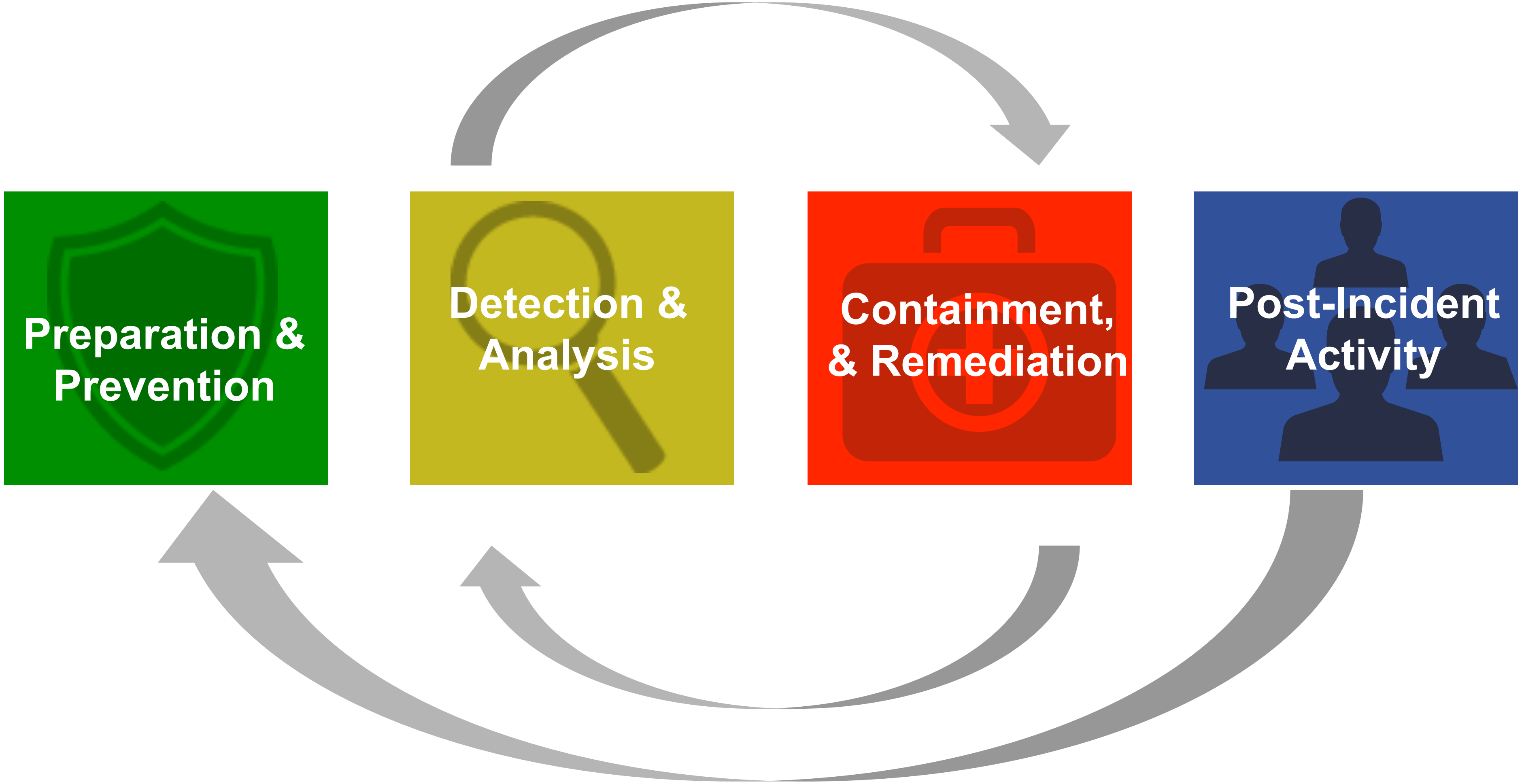
20 Critical Security Controls		NSA Rank
CSC1	Inventory H/W Assets, Criticality and Location	Very High
CSC2	Inventory S/W Assets, Criticality and Location	Very High
CSC3	Secure Configuration of Servers and Hardware	Very High
CSC4	Vulnerability Assessment and Remediation	Very High

NIST 800-53

Critical Security Control 10

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Incident Response Flow



Preparation & Prevention

Detection & Analysis

Containment, & Remediation

Post-Incident Activity

Vulnerability Identification

Preparation & Prevention

1) New high impact vulnerability hits
2) How quickly can you answer this question “What systems are impacted?”
3) Which of these affected systems are public facing?
4) Which systems are critical assets?
    1) What systems are critical for business continuity?
    2) What systems house sensitive data?

Patching

Preparation & Prevention

Patching for high impact vulnerabilities is different from routine patches from key vendors and distributions such as Linux distros, Microsoft, Oracle and Adobe for example.

Security teams need to ensure that the IT teams in their organization are able to quickly issue urgent patches. As per CSC 1& 2 this requires having an updated inventory of all systems applications, endpoints, servers, and other devices. IT and security teams need to be confident and have documentation for how to update these systems.

.

Detection & Analysis

After systems have been patched, there needs to be continuous monitoring of the environment for the vulnerability. When a new device is introduced to the environment it should automatically be scanned for this and other vulnerabilities.

IDS/IPS, Firewalls and Anti-Virus systems should all be updated to identify potential exploit signatures targeting the vulnerability in your environment.

Detection: Precursors and Indicator Sourcesx	
Alerts IDP/IPS SIEM/Log Intelligence Antivirus File Integrity Monitoring	**Third Party Threat Intelligence** Malware file hashes IP addresses Mutex Registry
Logs Operating systems, services and application Network device Network flow	**People** Employees & Contractors Business partners Customers & External parties Media

Containment,
& Remediation

- Between when the vulnerability was announced and systems were patched, systems may have been compromised, especially active exploits available
- Systems that were vulnerable and exposed should have any passwords changed and keys changed
- Systems should also be audited to detect any changes that were made while they were vulnerable for signs of intrusion/compromise.

Containment, & Remediation

- System configurations should also be compared to “gold standards” and if needed may need to be put back into a trusted state.

- If a system is believed to have been compromised, security teams should isolate the system

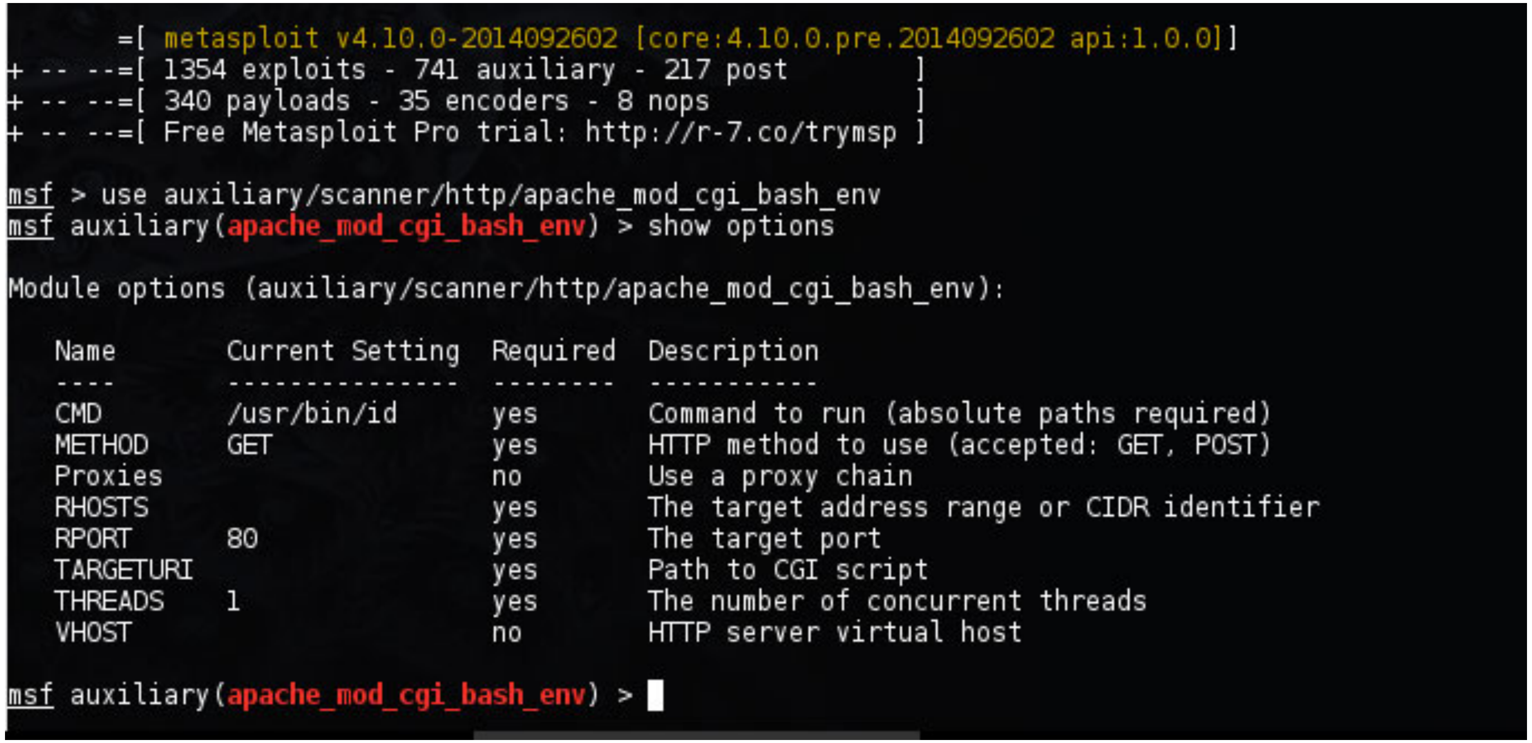
- If needed forensic procedures may need to be deployed to save an image of the compromised system before wiping or reinstating any systems.

- Note: Some compromised systems may need to say up but contained for business continuity.

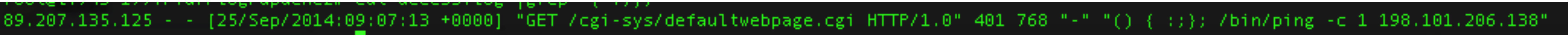
Post-Incident Activity

- After systems are patched and remediated, additional clean up and monitoring will be required.
- It is important to identify weaknesses in the response process whether it is technical or people oriented.
- Are there additional steps that can be take to improve both preventative measures, as well as increase response/remediation time?
- Can more of the process be automated?

Shellshock Exploit Indicators

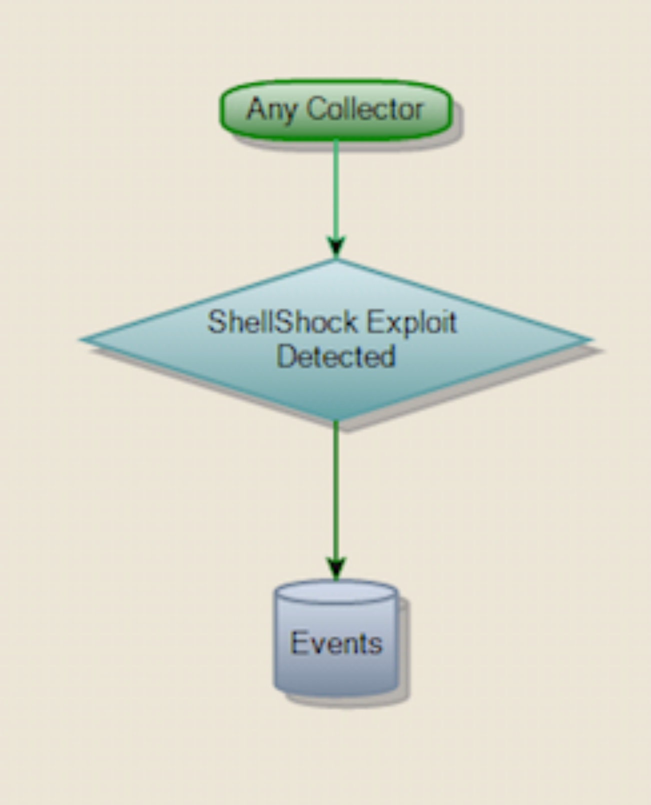


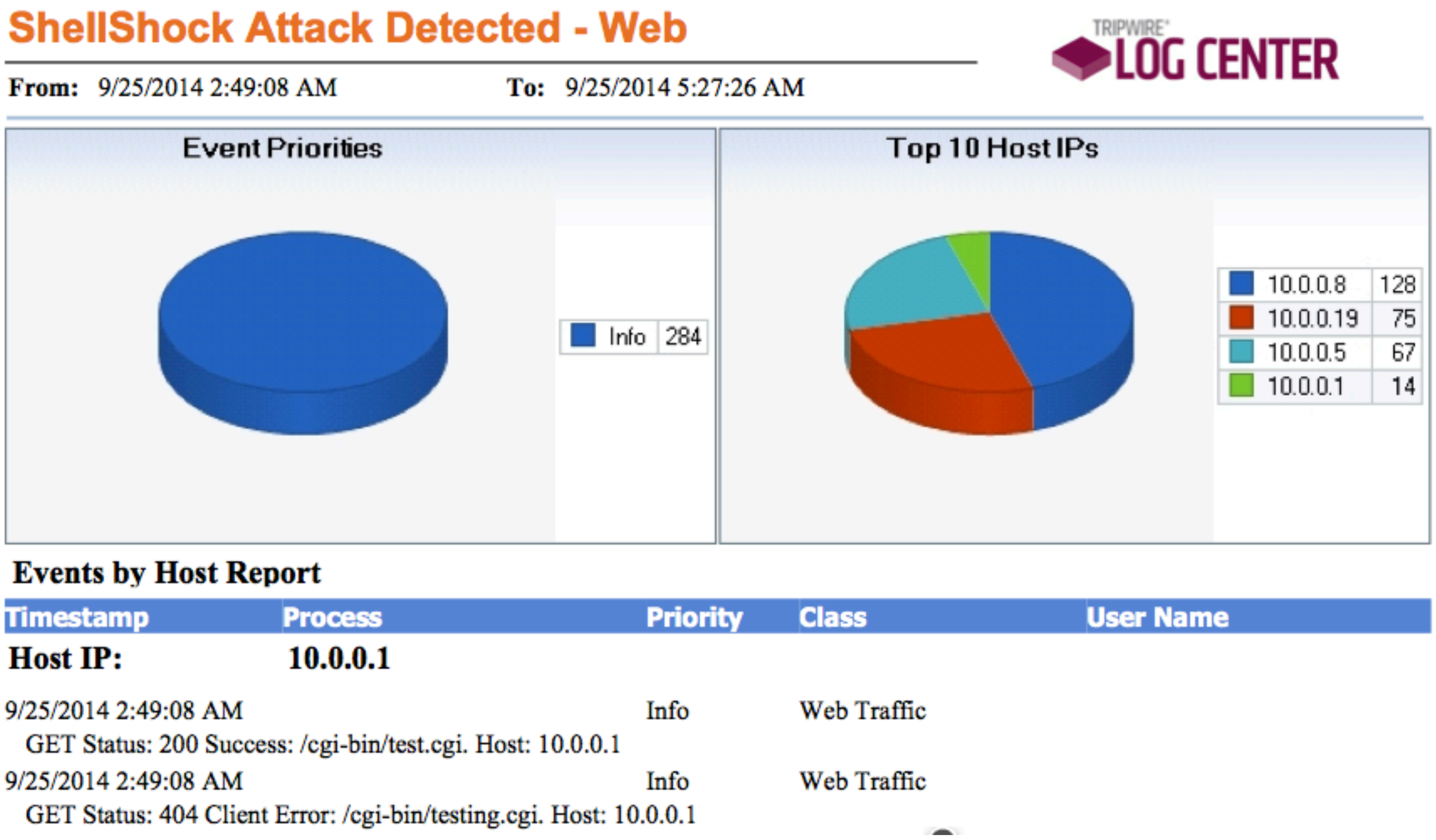
```
       =[ metasploit v4.10.0-2014092602 [core:4.10.0.pre.2014092602 api:1.0.0]]
+ -- --=[ 1354 exploits - 741 auxiliary - 217 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/http/apache_mod_cgi_bash_env
msf auxiliary(apache_mod_cgi_bash_env) > show options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CMD        /usr/bin/id      yes       Command to run (absolute paths required)
   METHOD     GET              yes       HTTP method to use (accepted: GET, POST)
   Proxies                     no        Use a proxy chain
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   TARGETURI                   yes       Path to CGI script
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf auxiliary(apache_mod_cgi_bash_env) > 
```



```
89.207.135.125 - - [25/Sep/2014:09:07:13 +0000] "GET /cgi-sys/defaultwebpage.cgi HTTP/1.0" 401 768 "-" "() { :;}; /bin/ping -c 1 198.101.206.138"
```

Shellshock Detection in Logs





ShellShock Attack Detected - Web

From: 9/25/2014 2:49:08 AM **To:** 9/25/2014 5:27:26 AM

Event Priorities

🟦 Info	284

Top 10 Host IPs

🟦 10.0.0.8	128
🟥 10.0.0.19	75
🟦 10.0.0.5	67
🟩 10.0.0.1	14

Events by Host Report

Timestamp	Process	Priority	Class	User Name
Host IP:	**10.0.0.1**			
9/25/2014 2:49:08 AM		Info	Web Traffic	
GET Status: 200 Success: /cgi-bin/test.cgi. Host: 10.0.0.1				
9/25/2014 2:49:08 AM		Info	Web Traffic	
GET Status: 404 Client Error: /cgi-bin/testing.cgi. Host: 10.0.0.1				

Heartbleed IDS Detection

March 21 10:23 – Google Security finds vulnerability

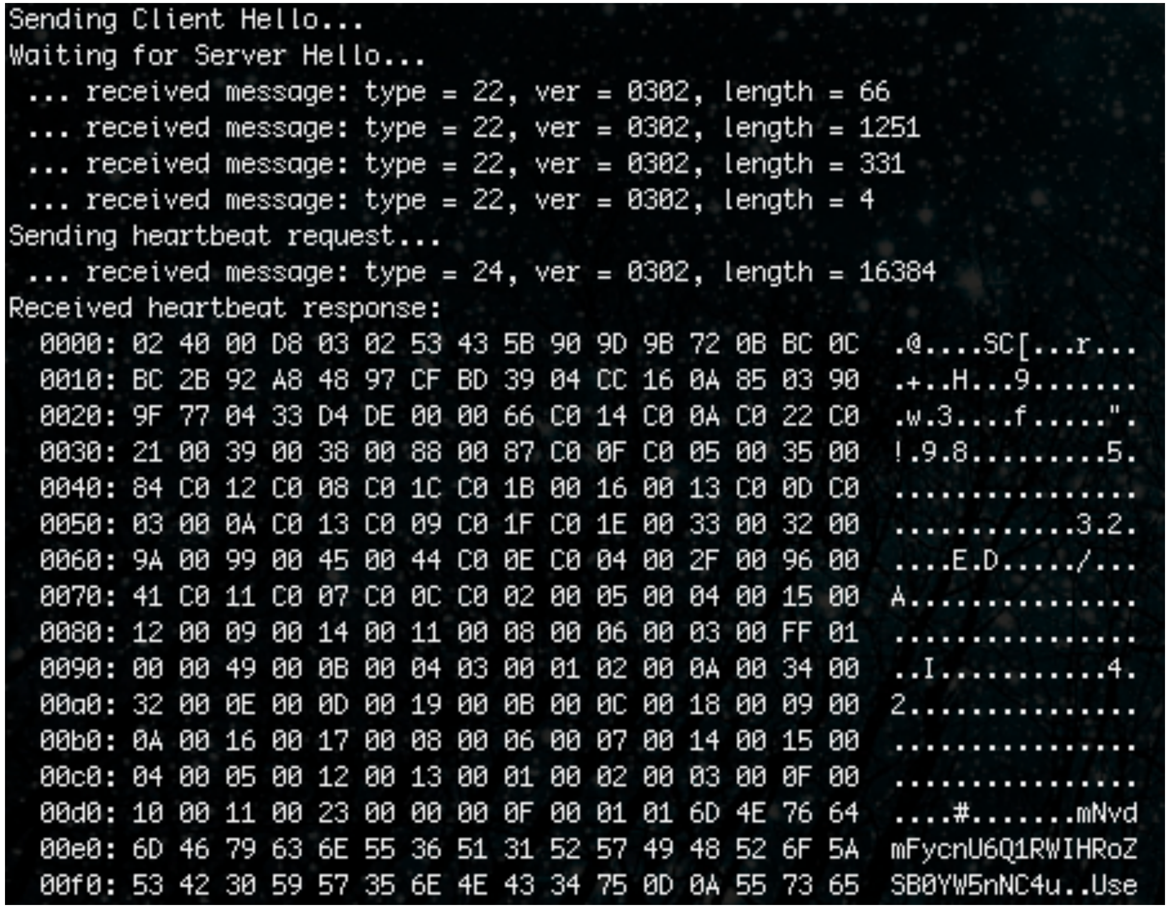
March 31- Cloudflare patches

April 1 - Google Security notifies OpenSSL a

April 7 – Open SSL patch available

April 12 – Exploits appear

April 16 – FBI releases Snort signatures



```
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 1251
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 6D 4E 76 64  ....#.......mNvd
  00e0: 6D 46 79 63 6E 55 36 51 31 52 57 49 48 52 6F 5A  mFycnU6Q1RWIHRoZ
  00f0: 53 42 30 59 57 35 6E 4E 43 34 75 0D 0A 55 73 65  SB0YW5nNC4u..Use
```

Thank You

Travis Smith

tsmith@tripwire.com