Vulnerability Alerting Program

Being effective in a diverse, decentralized environment

Curtis McNay
Director of IT Security
George Mason University
VA SCAN Conference 2010
Part of the mission of the IT Security Office is to alert the community of current threats.

- But the community is supporting one of everything. And we don’t know about everything that they’re supporting.
- Bombarding the community with general vulnerability alerts had the feeling and the effect of sending spam.
- Providing specific analysis and alerting is very time consuming.
Challenge continued..

- The process by which system administrators were receiving vulnerability notification was haphazard.
  - Vulnerability scan results from the IT security office.
  - Vendor and government list serves.
  - Security sites providing for alerts like SANS top 20 or USCERT’s Cyber Alerts.
- System Administrators needed system specific information when they could use it.
  - Vulnerabilities specific to the systems they were supporting.
  - When performing maintenance or otherwise evaluating their systems.
The Current Standard
NIST– National Vulnerability Database

- Provides a searchable database of current and historic known vulnerabilities.
  - Standards Based – Security Content Automation Protocol (SCAP)
    - CPE – Common Platform Enumeration
    - CVE– Common Vulnerabilities and Exposures
    - CVSS–Common Vulnerability Scoring System

- Provided by DHS, and is the standard that federal and local governments rely upon.
Search Engine..

National Vulnerability Database

Search CVE and CCE Vulnerability Database
(Advanced Search)

Keyword search: Apache

Search All
Search Last 3 Months
Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

- Software Flaws (CVE)
- Misconfigurations (CCE), under development

NVD now maps to CWE! See NVD CWE for more details.
Search Results (Refine Search)

There are 500 matching records. Displaying matches 1 through 20.

1 2 3 4 5 6 7 8 9 10 11 >>

CVE-2011-3368

Summary: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial '@' (at sign) character.

Published: 10/05/2011

CVSS Severity: 5.0 (MEDIUM)

CVE-2000-1247

Summary: The default configuration of the jserv-status handler in jserv.conf in Apache JServ 1.1.2 includes an "allow from 127.0.0.1" line, which allows local users to discover JDBC passwords or other sensitive information via a direct request to the jserv/ URI.

Published: 10/05/2011

CVSS Severity: 2.1 (LOW)
National Cyber-Alert System

Vulnerability Summary for CVE-2011-3368

Original release date: 10/05/2011
Last revised: 10/06/2011
Source: US-CERT/NIST

Overview
The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

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

References to Advisories, Solutions, and Tools
By selecting these links, you will be leaving NIST namespace. We have provided these links to other web sites because they may have information that would be of interest to you. No endorsement should be drawn as to other sites being referenced or not from this.
Advanced Search
While Useful, We Wanted More..

- An simple flexible search tool, that produced easy to use data for the IT Security Office and for the GMU Community.
- The ability to create searches that everyone would see.
  - Adobe, Oracle…. George Masons Top 20.
- The ability to create “unique to GMU” CVEs
  - Known appliances with vulnerable embedded XP
  - Common misconfigs: WordPress anonymous write privilege
- The ability to store specific comments with CVEs.
  - To site a policy, standard or resource.
- Customizable filters that users could created and stored.
  - Reflecting the uniqueness of the systems that they support.
And a Few other things

- A tool that a system or application administrator could use when they needed to.
  - When performing maintenance or otherwise evaluating their systems

- The ability to provide custom alert feeds to the different outlets where we have a presence.
  - IT Security web site alert page
  - IT Support web site alert page
  - “mymasonportal.gmu.edu” university portal
  - SALT Blackboard Organization Site
  - SALT list serve
What We’ve Come Up With.

<table>
<thead>
<tr>
<th>Vulnerability ID</th>
<th>Date Published</th>
<th>Software</th>
<th>Score</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2011-3287</td>
<td>06/06/2011 08:55:05</td>
<td>Cisco Jabber Extensible Communications Platform (aka Jabber)</td>
<td>7.8</td>
<td>Cisco Jabber Extensible Communications Platform (aka Jabber)</td>
</tr>
<tr>
<td>CVE-2011-3283</td>
<td>06/06/2011 08:55:05</td>
<td>Cisco Unified Presence 7.0%2013%20</td>
<td>7.8</td>
<td>Cisco Unified Presence before 8.5(4) does not properly detect</td>
</tr>
<tr>
<td>CVE-2011-3286</td>
<td>06/06/2011 08:55:05</td>
<td>Cisco Firewall Services Module</td>
<td>7.8</td>
<td>Cisco Firewall Services Module (aka FWSM) 3.1 before 3.1(4) does not</td>
</tr>
<tr>
<td>CVE-2011-3287</td>
<td>06/06/2011 08:55:05</td>
<td>Cisco Firewall Services Module</td>
<td>7.8</td>
<td>Cisco Firewall Services Module (aka FWSM) 3.1 before 3.1(4) does not</td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 4,269 entries (filtered from 4,321 total entries)
CVE Exploded View

<table>
<thead>
<tr>
<th>Vulnerability ID</th>
<th>Date Published</th>
<th>Software</th>
<th>Score</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-1582</td>
<td>02/05/2010</td>
<td>Microsoft Internet Information Services (IIS) 6.0</td>
<td>2.6</td>
<td>Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an “Inverse Lookup Log Corruption (ILLC)” issue.</td>
</tr>
</tbody>
</table>

Vulnerability Details for CVE-2003-1582

<table>
<thead>
<tr>
<th>Published Date</th>
<th>Modified Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-02-05 17:30:02.0</td>
<td>2010-02-08 00:00:00.0</td>
<td>Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an “Inverse Lookup Log Corruption (ILLC)” issue.</td>
</tr>
</tbody>
</table>

Scoring

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th>Access Vector</th>
<th>Access Complexity</th>
<th>Authentication</th>
<th>Confidentiality Impact</th>
<th>Integrity Impact</th>
<th>Availability Impact</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6</td>
<td>NETWORK</td>
<td>HIGH</td>
<td>NONE</td>
<td>NONE</td>
<td>PARTIAL</td>
<td>NONE</td>
<td><a href="http://nvd.nist.gov">http://nvd.nist.gov</a></td>
</tr>
</tbody>
</table>

Software

<table>
<thead>
<tr>
<th>Common Name</th>
<th>CPE Name</th>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
<th>Update</th>
<th>Edition</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Information Services (IIS) 6.0</td>
<td>cpe:/a:microsoft:iis:6.0</td>
<td>microsoft</td>
<td>iis</td>
<td>6.0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

References

<table>
<thead>
<tr>
<th>Source</th>
<th>Type</th>
<th>Text</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUGTRAQ</td>
<td>UNKNOWN</td>
<td>20030394 Log corruption on multiple webservers, log analyzers, ...</td>
<td><a href="http://www.securityfocus.com/archive/1/313867">http://www.securityfocus.com/archive/1/313867</a></td>
</tr>
</tbody>
</table>

Comments (0)
## Details for Vulnerability: CVE-2003-1582

### Vulnerability Information
- **ID:** CVE-2003-1582  
- **Published:** 2/5/10 5:30:02 PM,000  
- **Modified:** 2/8/10 12:00:00 AM,000

### Summary:
Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.

### Vulnerability Score
- **Score:** 2.6  
- **Access Vector:** NETWORK  
- **Complexity:** HIGH  
- **Confidentiality Impact:** NONE  
- **Integrity Impact:** PARTIAL  
- **Availability Impact:** NONE  
- **Authentication:** NONE  
- **Generated On:** 2/8/10 9:36:00 AM,000  
- **Source:** http://nvd.nist.gov

### Software
- **Microsoft Internet Information Services (IIS) 6.0**

### References
- **RITCTRAQ**

### Recommendations / Notes
- There are no recommendations or notes for this entry. Click on the edit icon to add one.
The Search Engine
Global Search Quick Filter
Select and Create Custom Filters
Vulnerability Reporting Tool
Application Architecture

- Developer: Adam Curtis, IT Security Office, GMU
- Web application primarily written in Java/JSP.
- The backend is written in Java and utilizes the Struts 2 framework.
- Hibernate is used for the ORM and connects to a MySQL database.
- The frontend is written in JSP with heavy use of JavaScript. Libraries used include jQuery, DataTables, and various other jQuery related plug-ins.
- Currently, the Vulnerability Reporting Tool is hosted on a Tomcat instance in a Linux environment, but is not OS dependent.
What We Hope to Achieve

- By providing a simple to use, customizable search engine that provides easy to use results, the practice of checking for vulnerabilities will be better adopted.
- The IT Security office’s mission of alerting the community will be more successful with less effort and less spam.

Questions?...
Contact: cmcnay@gmu.edu