security-assessment.com

# Vulnerability Advisory

| | |
|---|---|
| **Name** | Panda Security – Privilege Escalation |
| **Vendor Website** | http://www.pandasecurity.com/ |
| **Date Released** | 27/6/2016 |
| **Affected Software** | Panda Global Protection 2016 (16.1.2)<br>Panda Antivirus Pro 2016 (16.1.2)<br>Panda Small Business Protection (16.1.2)<br>Panda Internet Security 2016 (16.1.2) |
| **Testing Environment** | Windows 10 |
| **Researchers** | Ashraf Alharbi |

## Description

Multiple Panda Security products are vulnerable to local privilege escalation. As the USERS group has write permissions over the folder where the PSEvents.exe process is located, it is possible to execute malicious code as Local System.

## Exploitation

"PSEvents.exe" is scheduled to be executed every hour with SYSTEM Privileges. When executed, it tries to locate a number of DLLs in its local directory to be loaded. However, some of these DLLs don't exist. The following screenshot shows list of missing DLLs:

**Missing DLLs**

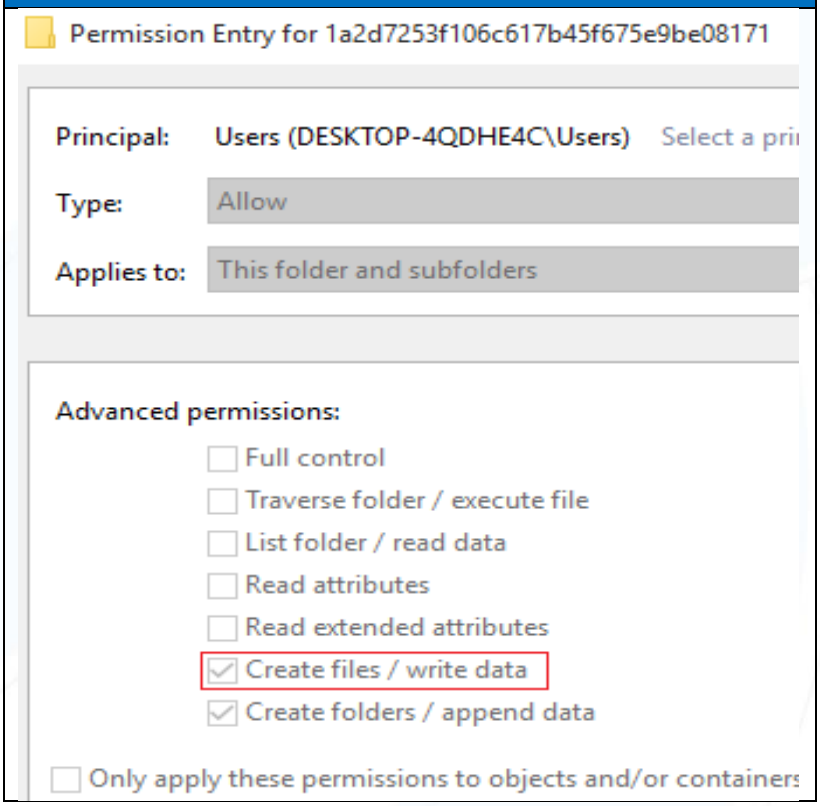
Path

C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\WINHTTP.dll
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\VERSION.dll
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\bcryptPrimitives.dll
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\PSEvents.exe.atc
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\default.atc
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\CRYPTBASE.dll
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\cryptnet.dll
C:\ProgramData\Panda Security\Panda Devices Agent\Downloads\1a2d7253f106c617b45f675e9be08171\WININET.dll

* The highlighted DLL name is going to be used later in this report

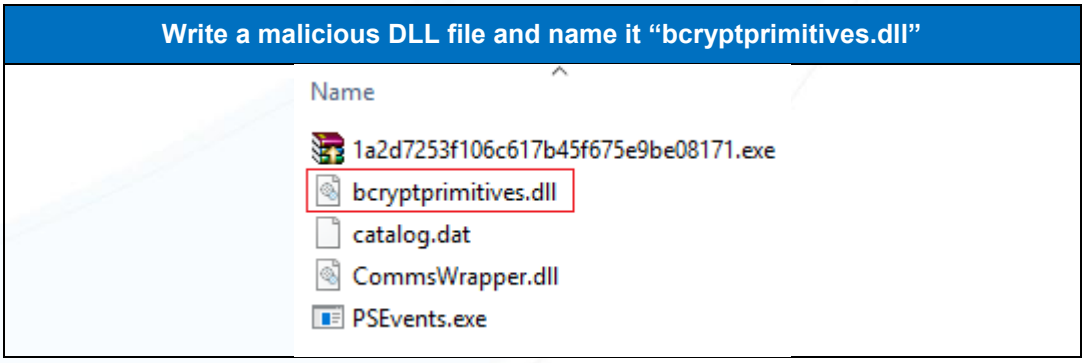
The DACLs of the directory that contains the "PSEvents.exe" executable allow a user in the USERS group to create files in that directory.

**DACLs for the directory that contains "PSEvents.exe"**



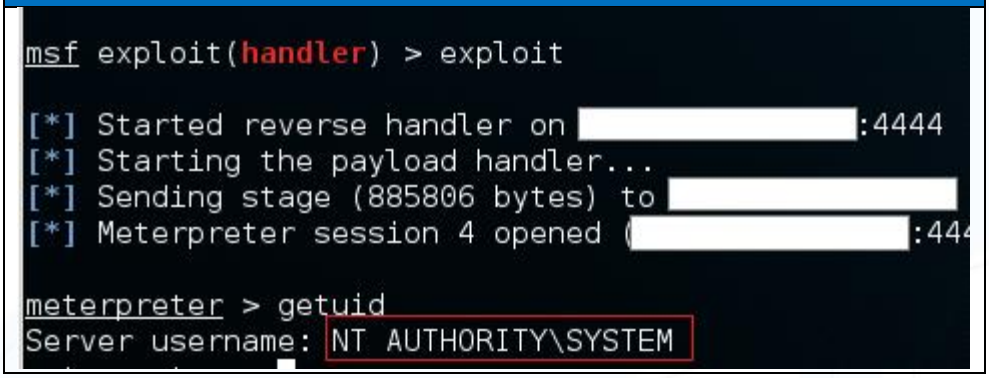

A malicious user can exploit this vulnerability by creating a malicious DLL file in that directory and name it as one of the missing DLLs. The following screenshots show the exploit details:

**Write a malicious DLL file and name it "bcryptprimitives.dll"**



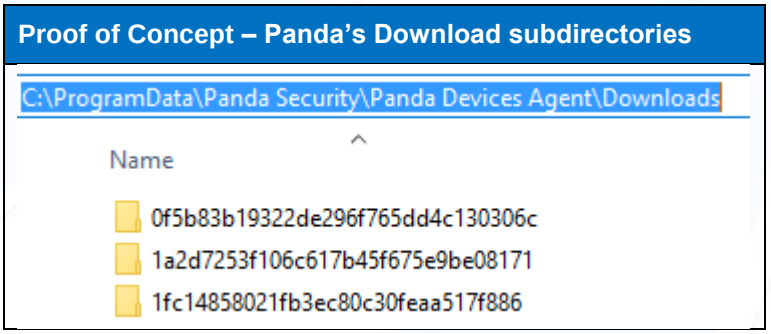
After one hour, the "PSEvents.exe" process will start and load our malicious DLL

**Proof of Concept – Reverse Shell running as SYSTEM**




The same method can be used to exploit other executables (PSDevice.exe and PSProfiler.exe) located in Panda's Downloads directory.

**Proof of Concept – Panda's Download subdirectories**




## Solution

Install Panda's Hotfix for this vulnerability.
http://www.pandasecurity.com/uk/support/card?id=100053

## Timeline

10/5/2016 - Exchange PGP
11/5/2016 - Advisory sent to Panda Security
14/5/2016 - Confirm receipt of the advisory
23/5/2016 - Email Panda Security for update
01/6/2016 - Panda Security reply that they have a fix in development.
16/6/2016 - Panda Security send hotfix to verify if it fixes the vulnerability.
21/6/2016 - Panda Security schedule to release the hotfix on 24/6/2016
24/6/2016 - Hotfix released
27/6/2016 - Advisory released

## About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and

government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com