Threat Modeling Report

Created on 11/10/2019 4:39:32 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	4
Needs Investigation	0
Mitigation Implemented	2
Total	6
Total Migrated	0

Diagram:

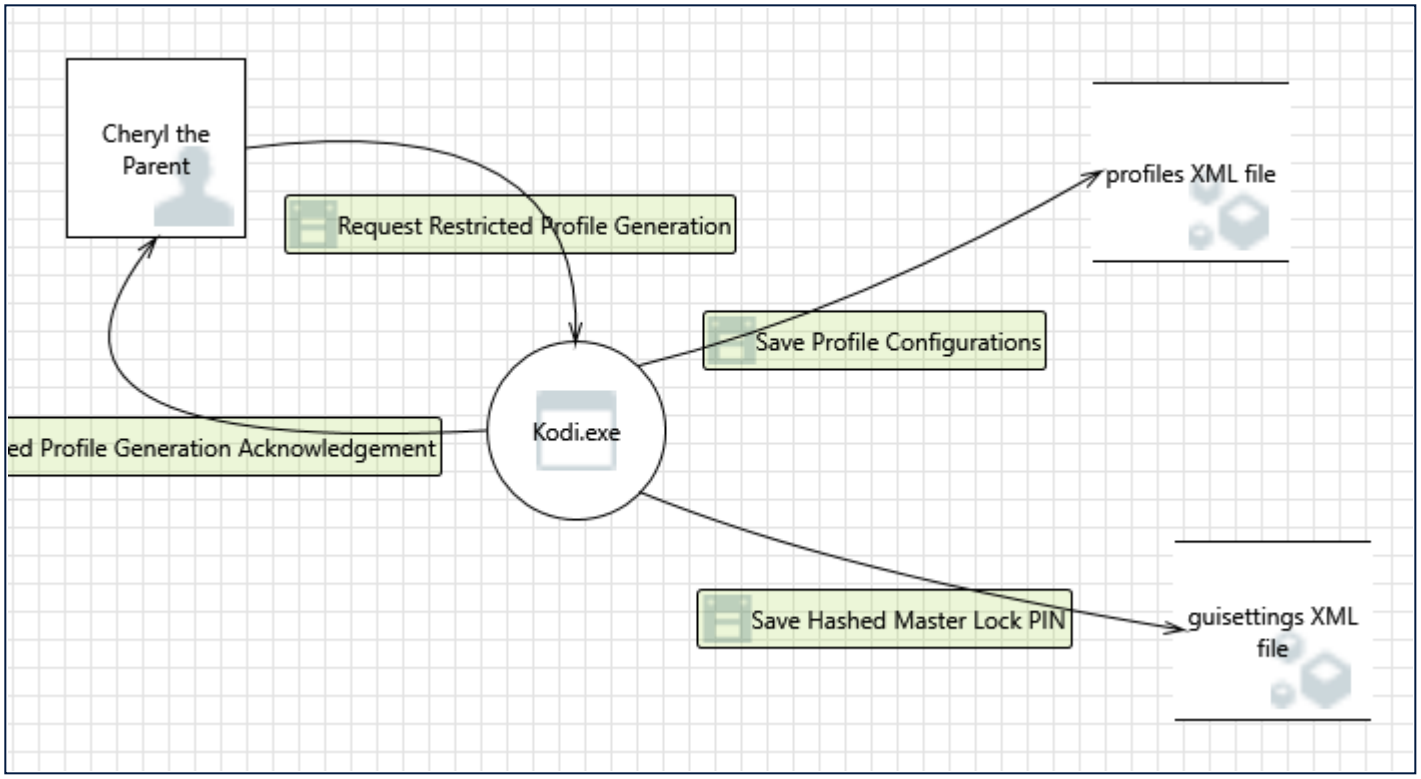
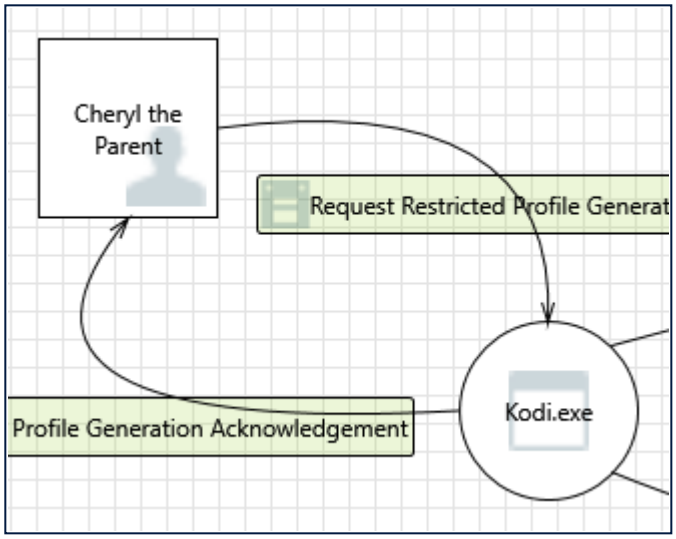


Diagram Summary:

Not Started	0
Not Applicable	4
Needs Investigation	0
Mitigation Implemented	2
Total	6
Total Migrated	0

Interaction: Request Restricted Profile Generation



1. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Kodi.exe may be able to impersonate the context of Cheryl the Parent in order to gain additional privilege.

Justification: The user can set up a Master Lock PIN to mitigate the potential of privilege escalation.

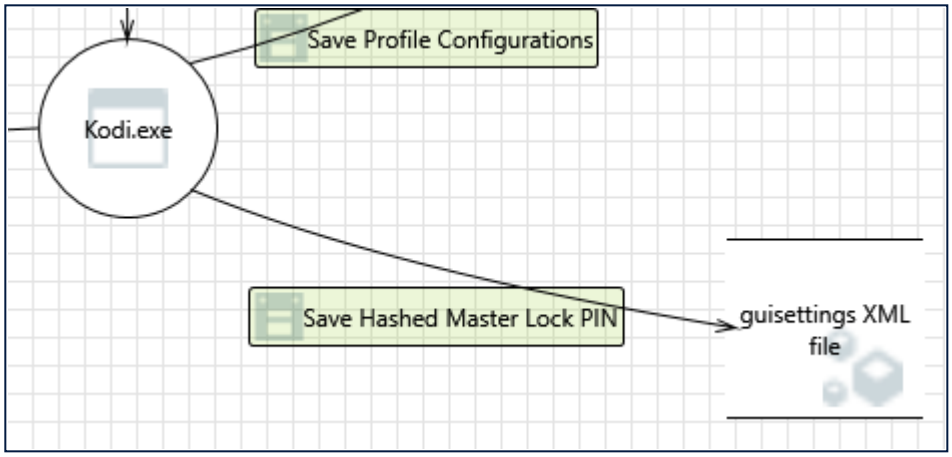
2. Spoofing the Cheryl the Parent External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Cheryl the Parent may be spoofed by an attacker and this may lead to unauthorized access to Kodi.exe. Consider using a standard authentication mechanism to identify the external entity.

Justification: Users may use PIN password to authenticate user profiles.

Interaction: Save Hashed Master Lock PIN



3. Potential Excessive Resource Consumption for Kodi.exe or guisettings XML file [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Kodi.exe or guisettings XML file take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: XML is stored on local hardware and is resource regulated by the operation system.

4. Spoofing of Destination Data Store guisettings XML file [State: Not Applicable] [Priority: High]

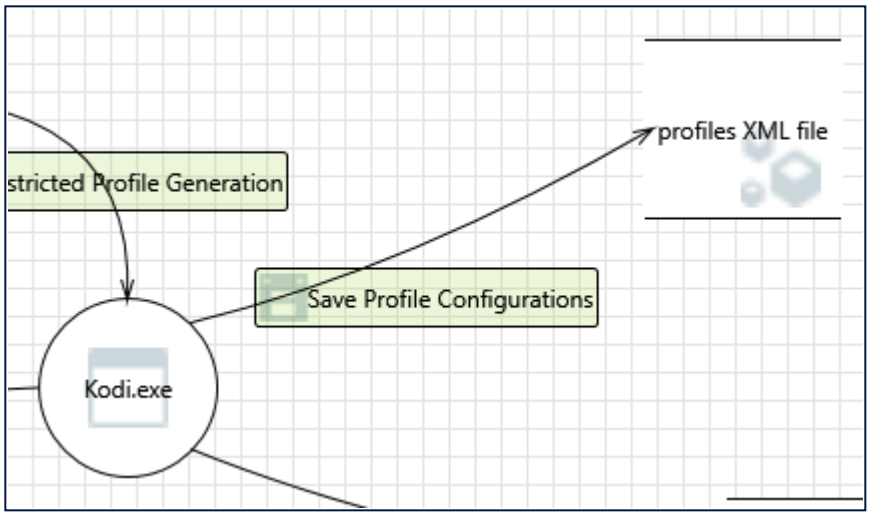
Category: Spoofing

Description: guisettings XML file may be spoofed by an attacker and this may lead to data being written to

the attacker's target instead of guisettings XML file. Consider using a standard authentication mechanism to identify the destination data store.

Justification: This file is stored locally on the user's hardware and filesystem. The filesystem is outside the scope of the process.

Interaction: Save Profile Configurations



5. Potential Excessive Resource Consumption for Kodi.exe or profiles XML file [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Kodi.exe or profiles XML file take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: XML is stored on local hardware and is resource regulated by the operation system.

6. Spoofing of Destination Data Store profiles XML file [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: profiles XML file may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of profiles XML file. Consider using a standard authentication mechanism to identify the destination data store.

Justification: This file is stored locally on the user's hardware and filesystem. The filesystem is outside the scope of the process.