Security Advisory- Polkit Privilege Escalation Vulnerability (CVE-2021-4034) - February 02, 2022

Overview
On January 25, 2022 a privilege escalation vulnerability (CVE-2021-4034) was found in Polkit's pkexec utility, part of a SUID-root program that is installed by default on all major Linux distributions, that allows unprivileged processes to communicate with privileged processes on Linux systems. The easily exploitable vulnerability allows a user with ordinary privileges to gain full root privileges on a vulnerable host in its default configuration. The vulnerability allows the user to bypass all authentication controls and policies due to incorrect handling of the process' argument vector.

References
- https://nvd.nist.gov/vuln/detail/CVE-2021-4034
- https://bugzilla.redhat.com/show_bug.cgi?id=2025869

Effective Security Severity Level
High

Affected Systems
All Ex Libris systems/products running on Linux.

Tests and Certifications
Ex Libris has evaluated all Ex Libris products for potential vulnerability and performed certification testing with the available patches for all Ex Libris systems and products running on Linux. It was determined that the available patches can be safely deployed with no impact to Ex Libris systems and products.

The fix for this vulnerability has been developed, tested, installed and certified for the Ex Libris Linux servers.

Action Taken by Ex Libris for Cloud Systems
Ex Libris has deployed the fix that addresses the vulnerability described in this advisory and no action is required by our cloud customers.

Required Actions for On-Premise/Local Systems
Ex Libris strongly recommends following the vendor's instructions and installing the patch on all on-premises (local) Ex
Libris products using Linux systems.

**Exploitation and Public Announcements**

The Ex Libris Security Incident Response Team (SIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

**Record of Changes**

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title:</td>
<td>Security Advisory – Polkit Privilege Escalation Vulnerability (CVE-2021-4034) - February 02, 2022</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Barak Rozenblat – VP Cloud Services</td>
</tr>
<tr>
<td>Issued:</td>
<td>February 02, 2022</td>
</tr>
<tr>
<td>Reviewed &amp; Revised:</td>
<td>February 02, 2022</td>
</tr>
</tbody>
</table>

**Revision Control**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Nature of Change</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version</td>
<td>February 02, 2022</td>
</tr>
</tbody>
</table>

**Document Distribution and Review**

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated regularly or upon written request by an approver or stakeholder. Questions or feedback about this document can be directed to the owner or a listed approver.