

Document ID AAGS-HOSP-SA-2022-001	Revision 3	Date 2022-01-26	Document category Security Advisory
Confidentiality level Public	Status Approved	Page (of) 1 (3)	

AAGS-HOSP-SA-2022-001 - PWNKIT

Hospitality

TLP:WHITE

Disclosure is not limited.

Overview

ASSA ABLOY Global Solutions Hospitality has investigated the vulnerability PwnKit (CVE-2021-4034) related to Linux privilege escalation.

This investigation followed our Product Security Incident Response (PSIR) Policy to identify affected products, assessing any potential implications for our customers, determine what mitigation steps should be taken, and notify affected customers.

Advisory Status

Investigation Done

While our product investigation is done, we will continue to monitor the threat environment and update this advisory if this situation changes. Our security teams are actively monitoring our environments and updated our defence-in-depth tools. We have no indication of any breach in our environment.

CLOUD PRODUCT & SERVICES

ASSA ABLOY Global Solutions Hospitality hosted solutions and services have been updated to fix this vulnerability in accordance with our patch process.

Document ID AAGS-HOSP-SA-2022-001	Revision 3	Date 2022-01-26	Document category Security Advisory
Confidentiality level Public	Status Approved		Page (of) 2 (3)

AFFECTED PRODUCTS

We have not found that the vulnerabilities impact our products.

Vulnerability Description

A local privilege escalation vulnerability was found on polkit's pkexec utility.

IMPACT

When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

SEVERITY

The CVSSv3.1 score for this vulnerability is:

7.8 (High) - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

REMEDIATION

No further mitigations are needed at customer property.

Contact Information

If you have any questions about this advisory, please contact our 24/7 support on +1 214-833-6778.

REFERENCES

- CVE-2021-4034 - <https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt>
- <https://nvd.nist.gov/vuln/detail/CVE-2021-4034>

REVISION HISTORY

Revision	Date	Description
1. 1	2022-01-26	Initial Publication
2. 2	2022-01-31	Investigation done, updated status
3. 3	2022-04-01	Structural changes to advisory for compliance

Document ID AAGS-HOSP-SA-2022-001	Revision 3	Date 2022-01-26	Document category Security Advisory
Confidentiality level Public	Status Approved		Page (of) 3 (3)

TERMS OF USE

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITTS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.