Security Advisory Report - OBSO-2202-01

pwnkit: Local Privilege Escalation in polkit's pkexec (CVE-2021-4034)

Release Date:	2022-01-29 19:31:01
Last Update:	2022-08-12 15:16:13
Version:	1.2

Summary

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according to predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

The vulnerability is rated high.

For **Atos Unify products that are considered appliances** and are using embedded linux operating systems we are evaluating the impact of our products

Atos Unify applications that are running on linux operation systems could be affected by this vulnerability. Customers are advised to follow the instructions of the operating system providers and apply the patches provided.

Atos Unify products that are running on windows operation systems are not affected.

Details

The Qualys Security Advisory provides additional information about the vulnerability.

The exploitation of the vulnerability requires that a local user account is compromised.

The CVVS 3.1 rating is 7.8
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Products

Atos Unify products that are considered appliances with an embedded linux operating systems are under investigation.

Atos **Unify applications that are installed on a linux operating systems** that is not embedded within the product are considered as **confirmed not affected.** Customer should follow the instructions of the linux operating system provider and apply the patches that are provided. Atos Unify will not deliver updates for linux based applications.

Atos Unify applications that are installed on Windows operating systems are not affected.

Products confirmed affected

Linux based appliances

Atos Unify OpenScape Voice (simplex deployments) V9 an V10 (hotfix provided in V9R4.48.16 (available), fixed in V10R2.14.0 (available)/ see OSV note)
Atos Unify OpenScape Voice (duplex deployments) V9 an V10 (hotfix provided in V9R4.48.16 (available), fixed in V10R2.14.0 (available) / see OSV note)
Atos Unify OpenScape First Response ESRP V9 (A hotfix is planned, see OSV note)
Atos Unify OpenScape Xpert Clients V6 and V7 (Fixed in V7 R4) (available)
Atos Unify OpenScape Contact Media Service V10,V11 up to V11 R0.0.2 (Fixed in V11 R0.1.0) (available)

Solutions and Cloud Services

Circuit (fixed in Sprint 164)
Atos Unify OpenScape Enterpise Express V9 and V10 (refer to OpenScape Voice evaluation)

Products confirmed not affected

Linux based appliances

Atos Unify OpenScape Business V3 (OpenScape Business X Systems)
Atos Unify OpenScape 4000 V8 and V10 Platform
Atos Unify OpenScape 4000 V8 and V10 Assistant
Atos Unify OpenScape 4000 V8 and V10 CSTA
Atos Unify OpenScape 4000 V8 and V10 Loadware
Atos Unify OpenScape Cordless IP V2
Atos Unify OpenScape First Response BCF V10
Atos Unify OpenScape First Response ESAAP V1
Atos Unify OpenScape Alarm Response Professional V4 and V5
Atos Unify Virtual Care Collaboration Service V1
Atos Unify OpenScape Branch V9 and V10
Atos Unify OpenScape SBC V9 and V10

Atos Unify OpenScape Desk Phones CP SIP
Atos Unify OpenScape Desk Phones CP HFA
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
OpenStage HFA V3
OpenStage SIP V3
Atos Unify OpenScape WLAN Phone WL3 and WL4
Atos Unify OpenScape DECT Phone S5 and S6
Atos Unify OpenScape DECT Phone SL5 and SL6
Atos Unify OpenScape WLAN Phone Wireless Service Gateway

Linux based applications ***(follow instructions of the linux operating system providers)***

Atos Unify OpenScape Business V3 (OpenScape Business S Server)
Atos Unify OpenScape First Response PSS V1
Atos Unify OpenScape First Response MSBF V2
Atos Unify OpenScape Xpert MLC V6 and V7
Atos Unify OpenScape UC Application V9 and V10
Atos Unify OpenScape 4000 Manager V8 and V10
Atos Unify OpenScape Common Management Platform V7 and V10
Atos Unify OpenScape Composer V2
Atos Unify OpenScape Voice Survival Authority
Atos Unify OpenScape Backup & Recovery Services

Applications that may be deployed on Windows or Linux (for Linux deployements check patches of linux providers)

HiPath CAP V3.0
Atos Unify OpenScape License Management CLA/CLM

Windows based applications

Atos Unify OpenScape Xpert System Manager V6 and V7
Atos Unify OpenScape Contact Center V10,V11
Atos Unify OpenScape Contact Center Extensions V3
Atos Unify OpenScape Fusion for Office V1 and V2
Atos Unify OpenScape Extensions for MS Outlook V1 and V2
Atos Unify OpenScape Fusion for Notes V1 and V2
Atos Unify OpenScape Web Collaboration V7
Atos Unify OpenScape Concierge V4
Atos Unify OpenScape Xpressions V7
Atos Unify OpenScape Personal Edition V7
Atos Unify OpenScape Deployment Service V7 and V10
Atos Unify OpenScape Fault Management V10, V11 and V12
Atos Unify OpenScape Accounting Management V3, V4 and V5
Atos Unify OpenScape Voice Trace Manager V8

AC Win SL V3
HiPath DS-Win V4
Atos Unify OpenScape Sesap V2

Products under investigation

Atos Unify OpenScape First GEMMA V2 and V3

Additional notes for planned fixes and updates:

OpenScape Voice V9 and V10 (simplex and duplex deployments) and OpenScape First Response ESRP V9

- A hotfix is planned that implements the workaround sugested by Suse

Recommended Actions

Available workarounds:

For Linux based appliances

Currently no workarounds are available.

For Atos Unify applications using affected linux operating systems:

- Check operatng systems providers recommendation
- Apply the patches that are provided

References

External References

- https://nvd.nist.gov/vuln/detail/CVE-2021-4034
- https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
- https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
- https://security-tracker.debian.org/tracker/CVE-2021-4034
- https://ubuntu.com/security/CVE-2021-4034
- https://www.suse.com/security/cve/CVE-2021-4034.html
- https://www.suse.com/support/kb/doc/?id=000020564

Version Change History

Version	Date	Description
1.0	03.02.2022	- Initial release
1.1	18.05.2022	- OpenScape Voice hotfix V9R4.48.16 (available), hotfix planned in V10R2.14.0 for 08/2022 - OpenScape Contact Media Service fixed in V11 R0.1.0 - OpenScape Xpert Clients fixed in V7 R4
1.2	12.08.2022	- OpenScape Voice fixed in V10R2.14.0

Advisory: OBSO-2202-01, status: update release
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.