Security Bulletin:

PwnKit affecting SMC CVE-2021-4034

Author : Atos BDS TI Team
Created : 2022-01-27
Last Update : 2022-05-30
Revision : 2.0
Keywords :

TLP:WHITE

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

REVISION: 2.0 **PUBLIC** **TLP:WHITE**

Executive summary

Users of the Atos Smart Management software suite should upgrade polkit component as soon as possible.

A vulnerability in Polkit's pkexec component identified as CVE-2021-4034 (PwnKit) is present in the default configuration of all major Linux distributions and can be exploited to gain full root privileges on the system. Trivial exploits are available on the internet.

The component polkit may be used on some systems as an alternative to sudo. It is not installed by default on Atos servers.

Due to the ease of the exploitation, it is recommended to double check that the component is not installed, and to upgrade or remove it, if found.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2021-4034	7.4	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C

Affected products

The polkit package is not part of the default configuration of Atos products.

Atos Product line	Version	Status	Comments
SCS5 Management Center	Release R3	affected	The vulnerable component is used as a dependency of others. Atos has validated the compatibility of the latest version with RHEL 7.9 and RHEL 8.5, which are the supported RedHat versions. Upgrading to the latest versions of RHEL 7.9 and 8.5 fixes the vulnerability.
SMC	SMC 1.2.6	affected	The vulnerable component is used as a dependency of others. Atos has validated the compatibility of the latest version with RHEL 7.9 and RHEL 8.5, which are the supported RedHat versions. Upgrading to the latest versions of RHEL 7.9 and 8.5 fixes the vulnerability.
SMC xScale	xScale 1.0.6	affected	The vulnerable component is used as a dependency of others. Atos has validated the compatibility of the latest version with RHEL 7.9 and RHEL 8.5, which are the supported RedHat versions. Upgrading to the latest versions of RHEL 7.9 and 8.5 fixes the vulnerability. Note: ETA for RHEL 8.5 compatibility is 2022/02/04
BullSequana X		Not affected	The vulnerable component is not embedded in BMC.
BullSequana S		Not affected	The vulnerable component is not embedded in BMC.
BullSequana Edge		Not affected	The vulnerable component is not embedded in BMC.

Although ATOS makes effort to provide accurate and complete information, ATOS shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

Recommendations

Check for the presence of pkexec executable. It is usually located in /usr/bin.

Upgrade polkit package, if present, using your Linux distribution repositories.

Available Vendor Patches

The updated Redhat packages will be incorporated in Atos repositories for download.

The polkit project has a dedicated patch: https://gitlab.freedesktop.org/polkit/polkit/-/issues/166

Available Workarounds

RedHat has published some possible workaround to mitigate the risk in case polkit must remain in use. Please refer to [2].

Another workaround is to remove setuid bit on the executable

```
chmod 755 /usr/bin/pkexec
```

Caution: This workaround has unpredictable impact on the applications which rely on pkexec to acquire some capabilities or rights. Testing of the workaround impact out of production is recommended.

When polkit resides on a read-only filesystem, the following trick can also disable the pkexec executable with the same kind of unpredictable impact.

1. Create an executable bash script on a writable filesystem
```
cat > /path/to/pkexec.overmount <<EOF
#!/bin/bash

echo "/usr/bin/pkexec has been disabled"
exit 1
EOF
```
2. Make script executable
```
chmod 755 /path/to/pkexec.overmount
```
3. Overmount the script on the vulnerable executable
```
mount -o bind /path/to/pkexec.overmount /usr/bin/pkexec
```

Available Mitigations

The exploit needs an existing legitimate user access to get elevated (system) privileges.

Available Exploits/PoC

Exploitation in the wild of the vulnerability has been observed. Exploits are freely available to check the vulnerability (e.g. https://github.com/berdav/CVE-2021-4034)

References

1. https://access.redhat.com/security/cve/CVE-2021-4034
2. https://access.redhat.com/security/vulnerabilities/RHSB-2022-001

3. https://www.thesecmaster.com/how-to-fix-the-polkit-privilege-escalation-vulnerability-cve-2021-4034/

List of changes

Version	Date	Description
0.1	27/01/2022	First neutralization version.
0.2	28/01/2022	Add statement that Smart Management Center and related products are affected. Proposed workaround for read-only/diskless situations.
0.3	28/01/2022	Add simple setuid workaround and warning on potential unpredictable impact.
1.0	31/01/2022	First remediation version. Clarification on the Smart Management Center versions which are confirmed compatible with the fix.
2.0	30/05/2022	Public version.

Glossary of terms

Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability.
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated. Security bulletins issued during this phase are numbered 0.x.
POC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression. Security bulletins issued during this phase are numbered 1.x when private. Publicly disclosed bulletins are numbered 2.x.
TI	Threat Intelligence
TLP	Traffic Light Protocol
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update.

About this document

ATOS continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the Traffic Light Protocol (TLP)[1] to bring attention of owners of the potentially affected ATOS products. ATOS recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although ATOS makes effort to provide accurate and complete information, ATOS shall not be liable for technical or editorial errors contained in this Bulletin. The information provides is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither ATOS nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Product and company names mentioned herein may be trademarks of their respective owners.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea), listed on Euronext Paris and included on the CAC 40 ESG and Next 20 Paris Stock Indexes.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

[1] https://www.cisa.gov/tlp