EVIDEN
an atos business

Security Bulletin

CardOS API Local Privilege Escalation

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-358**
Created	:	**14 November 2023**
Version	:	**2.6**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**22 March 2024**
Keywords	:	**CVE-2023-41099**

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

FOR PUBLIC USE

List of changes

Version	Date	Description
~~0.1~~ D.0	2023/08/30	First draft version
~~0.2~~ 0.1	2023/08/31	First neutralization version
0.2	2023/11/14	Renumbering to fit with new Eviden template
1.3	2023/11/15	First remediation version
1.4	2023/12/17	Adding internal PSIRT reference
1.5	2024/03/05	Relaxing confidentiality for sharing
2.6	2024/03/22	Removing details for public disclosure of the vulnerability

Executive summary

A vulnerability has been discovered internally on the Eviden CardOS API Windows installer. It allows Local Privilege Escalation from regular user to SYSTEM.

This Privilege Escalation doesn't provide significant additional risk if Standard Users have Local Administrative Privilege.

Eviden recommends updating the CardOS API Windows installer.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-41099	7.8	Local Privilege Escalation AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

This vulnerability applies to systems where CardOS API is already installed. It allows local privilege escalation.

Affected products

Although Eviden makes efforts to provide accurate and complete information, Eviden 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.

Products	Fixed version	Status	Comments
Atos CardOS API	5.5.5.2811	Affected version 5.x	The vulnerability was introduced in this branch by a change in package installer solution

Recommendations

Uninstall and Reinstall Atos CardOS API with version 5.5.5.2811 or later.

The uninstallation ensures removal of previously vulnerable MSI file.

Available Vendor Patches

The patched version 5.5.5.2811 of Atos CardOS API will be available to your usual customer support.

Available Workarounds

Disable the capacity for Standard Users to run MSI files.

Available Mitigations

This Privilege Escalation doesn't provide significant additional risk if Standard Users have Local Administrative Privilege.

Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

Acknowledgement

We wish to thank Julian HOROSZKIEWICZ from internal EVIDEN Red Team for his discovery.

References

1. https://learn.microsoft.com/en-us/windows/win32/msi/disablemsi

Glossary of terms

Term	Description
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.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
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

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden makes effort to provide accurate and complete information, Eviden 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 Eviden 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. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- https://support.bull.com/ols/product/security/psirt

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 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) and listed on Euronext Paris.

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.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.