an atos business

Security Bulletin

Potential privilege escalation in IDPKI

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1335
Created	:	08 June 2024
Version	:	2.10
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	30 January 2025
Keywords	:	CVE-2024-39327 CVE-2024-39328 CVE-2024-51505

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	2024/06/07	Initial Eviden bulletin
0.2	2024/06/21	Vulnerability ND-2 Added (later CVE-2024-39328)
0.3	2024/06/24	Relaxation of TLP level (TLP:AMBER). Use of CVE numbers assigned by Mitre.
0.4	2024/07/04	Detection script added. Backport of IDRA fix on older versions.
0.5	2024/09/02	Clarification of the impact on SaaS implementations.
0.6	2024/09/26	For CVE-2024-39328 – embargo date: end of January 2025 (publication of vulnerability) – waiting for TS
0.7	2024/10/29	Adding version information regarding CVE-2024-39328. Adding new vulnerability as revealed during validation.
0.8	2024/10/31	Adding CVE-2024-51505
1.9	2025/01/10	Version 2.7.1 with complete fix. Remediation version TLP:GREEN
2.10	2025/01/30	TLP:CLEAR version

Executive summary

A security assessment of IDPKI implementation revealed a weakness potentially allowing an operator to exceed its privileges.

Vulnerability Info

In the course of a pentest security assessment of IDPKI, some security measures protecting internal communications were found potentially compromised for an internal user with high privileges.

None of these vulnerabilities put Certificate Authority (CA) private key at risk.

Eviden analyzed the root cause of the weakness. It revealed two separate vulnerabilities. During validation of the fix, an additional vulnerability of similar nature was identified, leveraging some race condition to alter an internal automata state and achieve a system privilege escalation:

1. CVE-2024-39327: The vulnerability could allow the possibility to obtain CA signing in an illegitimate way.
2. CVE-2024-39328: Highly trusted role (Config Admin) could exceed their configuration privileges in a multi-partition environment and access some confidential data. Data integrity and availability is not at risk.
3. CVE-2024-51505: Highly trusted role (Config Admin) could leverage a race condition to escalate privileges.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-39327	9.4	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C
CVE-2024-39328	6.6	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:H/RL:T/RC:C
CVE-2024-51505	7.6	AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C

CVE-2024-39327 correction has been validated and published.

CVE-2024-39328 correction has been validated and published. This vulnerability has no impact in mono-partition nor in SaaS environments.

CVE-2024-51505 risk is increased if the last fixes are not applied, as a lower privileged role is required. A fix is available and published.

Affected products

Products	Fixed version	Status	Comments
IDRA	2.7.1	Fixed	CVE-2024-39327 Fixes released starting on 2024/06/21. CVE-2024-39328 Fixes released on 2024/10/03. CVE-2024-51505 Fixes released on 2024/11/08.
IDRA SaaS	2.7.1	Fixed	CVE-2024-39327 fixed by 2.6.1 on 2024/07/01. CVE-2024-39328 and CVE-2024-51505 are not affecting SaaS implementation due to attributed roles. CVE-2024-39328 is nevertheless fixed by version 2.7.0. CVE-2024-51505 is nevertheless fixed by version 2.7.1.
IDCA	2.7.0	Fixed	Not affected by CVE-2024-39327 nor CVE-2024-51505. Fix for CVE-2024-39328 released on 2024/10/03.
IDCA SaaS	2.7.0	Not affected	Not affected by CVE-2024-39327 nor CVE-2024-51505. CVE-2024-39328 is not affecting SaaS implementation due to attributed roles. CVE-2024-39328 is nevertheless fixed by version 2.7.0.

Although Eviden tries 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.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

Recommendations

CVE-2024-39327: Eviden recommends patching as soon as possible. A script and documentation are available to customers to detect if an exploit has occurred. It is also strongly recommended to renew the internal technical sensitive data which has been potentially exposed (see documentation).

CVE-2024-39328: Eviden recommends patching as soon as possible.

CVE-2024-51505: Eviden recommends patching IDRA as soon as possible.

Available Vendor Patches

Validated patch is available for CVE-2024-39327, CVE-2024-39328 and CVE-2024-51505. Support resources for IDnomic products are reminded in the table below.

Products	Technical State link
IDRA IDCA	https://support.idnomic.com/

Available Workarounds

Eviden recommends limiting Config Admin role to highly trusted users.

Available Mitigations

CVE-2024-39327: The exploitation of the weakness is normally mitigated by fine tune access to IDCA Web Services.

CVE-2024-39328: The exploitation of the weakness is mitigated because it is exposed only for highly trusted roles (Config Admin) in multi-partitioning environment.

CVE-2024-51505: The exploitation of the weakness is mitigated because it is exposed only for highly trusted roles (Config Admin).

Available Exploits/PoC

To analyze if the vulnerability CVE-2024-39327 has been exploited, a script and documentation are available to customers.

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

References

1. https://nvd.nist.gov/vuln/detail/CVE-2024-39327
2. https://nvd.nist.gov/vuln/detail/CVE-2024-39328
3. https://nvd.nist.gov/vuln/detail/CVE-2024-51505

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 the 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 tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information 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 Europapea) 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, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.