

## Security Bulletin

# Multiple Critical Vulnerabilities in iCare

Author(s) : Eviden PSIRT  
Reference : PSIRT-625  
Created : 07 February 2024  
Version : 0.7  
Status : Neutralization  
TLP Classification : CLEAR  
Document date : 30 August 2024  
Keywords : CVE-2024-42017

### **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	2023/11/13	Initial neutralization version
0.2	2023/11/16	Consolidated neutralization version
0.3	2023/12/17	Added internal PSIRT reference
0.4	2024/02/07	TLP changed for GREEN
0.5	2024/07/12	Added version 2.7.11
0.6	2024/08/29	CVE id added
0.7	2024/08/30	TLP changed

## Executive summary

During routine operations of its internal Red Team, Eviden discovered critical vulnerabilities in its iCare product.

This product is an administrative tool to manage the hardware of several servers of the Bullion S and BullSequana S family. Its goal is to ease firmware patching and server sensors monitoring. It runs on Windows or Linux and manage servers through the IPMI protocol.

Given the obsolescence of the product, it was decided not to patch the vulnerabilities, and to help our customers in migrating to other administrative solutions.

The application exposes a web interface locally. In the worst-case scenario, if the application is remotely accessible, it allows an opponent to execute arbitrary commands with system privilege on the endpoint hosting the application, without any authentication.

## Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-42017	10	Authorization Bypass Local Privilege Escalation Remote Command Execution <a href="#">AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H</a>

## Affected products

As versions 2.7.1 and 2.7.10 were tested vulnerable, it is likely that all versions of iCare shipped with Bullion S and BullSequana S technical states are vulnerable. This includes version 2.7.11 delivered with the latest BullSequana S TS74.02. There is no plan to fix these vulnerabilities.

## Recommendations

Eviden recommends to deinstall unused iCare from any system, Windows or Linux, as soon as possible.

## Available Vendor Patches

As this tool is leveraging obsolete technologies, the vulnerabilities won't be fixed. Eviden hereby declares the End-of-Life / End-of-Support of the iCare product.

## Available Workarounds

In case the immediate deinstallation of iCare is not possible for operational reasons, a host or virtual machine should be dedicated to its usage. The access to the host should be local and restricted to administrator level, or protected by means external to the host (firewall). If the tool is only used for firmware upgrade, the dedicated resource can also be powered on demand of a legitimate user.

## Available Mitigations

The application runs usually on port 12080. In general, this port is not accessible from the internet as soon as some firewalling techniques are in place. It is also likely that the tool is part of an isolated management network, which is also part of usual best practices.

An endpoint detection and response (EDR) agent is also able to mitigate the risk posed by iCare.

## Available Exploits/PoC

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

The vulnerabilities were discovered and exploited by Eviden internal Red Team during routine security control operations.

## Acknowledgement

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

## 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. <a href="https://www.first.org/tlp/">https://www.first.org/tlp/</a>
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 provided 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<sup>1</sup>

[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 5 billion.

---

<sup>1</sup> 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.

Eviden is a registered trademark. © Eviden SAS, 2024.