EVIDEN
an atos business

# Security Bulletin

# IPMI 2.0 RAKP Authentication Remote Password (SHC)

| | | |
|---|---|---|
| **Author(s)** | **:** | **Eviden PSIRT** |
| **Reference** | **:** | **PSIRT-645** |
| **Created** | **:** | **23 November 2023** |
| **Version** | **:** | **0.3** |
| **Status** | **:** | **Neutralization** |
| **TLP Classification** | **:** | **CLEAR** |
| **Document date** | **:** | **3 May 2024** |
| **Keywords** | **:** | **CVE-2013-4037 CVE-2013-4786** |

**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 | 2023/12/12 | Initial neutralization version |
| 0.2 | 2023/12/14 | Added synthetic sentence to executive summary<br>Proposed CWE for CVE-2013-4037.<br>Added reference to CISA's recommendations.<br>TLP:GREEN |
| 0.3 | 2024/05/03 | TLP:CLEAR and adding note on Bullion S EOL/EOS |

## Executive summary

IPMI (Intelligent Platform Management Interface) is a set of standardized specifications for hardware-based platform management systems that makes it possible to control and monitor servers centrally. It was first introduced in 1998 and, despite some improvements, the IPMI protocol suffers some design security flaws. Therefore, the more secure Redfish interface should be used if possible. In case IPMI interface is in use, its access should be restricted to a properly isolated management network.

CVE-2013-4786

The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the hash-based message authentication code (HMAC) from a RAKP message 2 response from a BMC.

CVE-2013-4037

The Remote Authenticated Key-Exchange Protocol (RAKP), which is specified by the IPMI standard for authentication, has flaws. Although the system does not allow the use of null passwords, a hacker might reverse engineer the RAKP transactions to determine a password. The authentication process for IPMI requires the management controller to send a hash of the requested password of the user to the client before the client authenticates. This process is a key part of the IPMI specification. The password hash can be broken by using an offline brute force or dictionary attack.

## Vulnerability Info

| CVE No. | CVSS Score | Type of Vulnerability |
|---|---|---|
| CVE-2013-4786 | 7.5 | CWE-255 - Credentials Management Errors |
| CVE-2013-4037 | N/A | CWE-327 - Use of a Broken or Risky Cryptographic Algorithm |

## Affected products

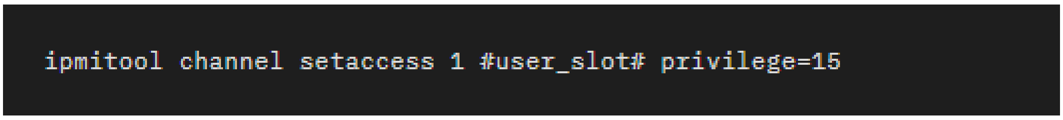
| Products | Fixed version | Status | Comments |
|---|---|---|---|
| Bullion S | N/A | Affected | Bullion S is out-of-support |
| Bullsequana S | N/A | Affected | No plan to fix |

Although Eviden makes effort 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.

## Recommendations

As those vulnerabilities are intrinsic to the IPMI protocol, no patch is envisioned. Only external protective recommendations can be applicable. Configuration options and best practices for these two vulnerabilities such as changing the preconfigured username and password when the server is deployed. This action prevents unauthorized users from gaining access to the system through the preconfigured user account.

If a user is not managing a server by using the IPMI, you can configure the system to disallow IPMI network access from the user accounts. This task can be accomplished by using the IPMItool utility or a similar utility for managing and configuring the IPMI management controllers. You can use the following IPMItool command to disable the network access for an IPMI user:



```
ipmitool channel setaccess 1 #user_slot# privilege=15
```

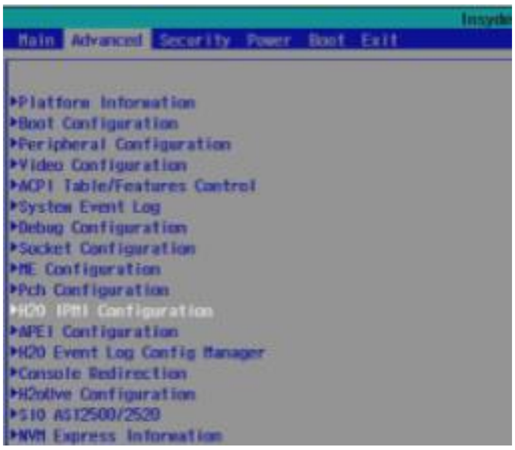
Executing the command directly on the server is demonstrated in this instance. However, if the IPMItool command is executed remotely over the network or if an alternative utility is employed, the command may differ. To ascertain the correct command syntax, refer to the documentation of the utility in use. By disabling IPMI network access, the vulnerability in the IPMI RAKP protocol that enables the discovery of user account credentials is eliminated.

It is highly recommended to create robust passwords that consist of a minimum of 16 characters, including a combination of uppercase and lowercase letters, numbers, and special characters. By opting for more intricate passwords, it becomes increasingly challenging for malicious individuals to gain access to legitimate user credentials.

It is advisable to maintain a distinct management network that is separate from the public network. By doing so, the security risks are minimized as the number of individuals with access to the systems is reduced.

## How to disable IPMI protocol:

In BIOS settings, the IPMI configuration is present on “advanced” BIOS page and “H2O IPMI configuration:



Set the “IPMI Support” value to “disabled”.

**Caution! Disabling IPMI prevents to manage the servers by tools such as BMSCli and iCare.**

## For Bullion servers :

BSMCli command can be used to disable IPMI:

- Command to set "IpmiEnable" (0 ipmi disable - 1 ipmi enable):

```
/opt/BSMHW_NG/bin/bsmBiosSettings.sh -H 129.182.202.4 -u
super -p pass -a set -n 'IpmiEnable 0'
Setting IpmiEnable is OK
```

- Command to check "IpmiEnable" setting:

```
/opt/BSMHW_NG/bin/bsmBiosSettings.sh -H 129.182.202.4 -u
super -p pass -a get -n 'IpmiEnable'
IpmiEnable       : 0
```

## For BullSequana servers :

IPMI can be disable by using the SHC Gui:

Configuration -> BMC Settings -> Network : <Disable IPMI Protocol over LAN>

## Available Vendor Patches

No patch will be made available.

Technical States links for Eviden servers are reminded in the table below.

| Product | Technical State link |
|---|---|
| Bullion S | https://support.bull.com/ols/product/platforms/bullion/bullion-S/dl/pkgf/pkg |
| Bull Sequana S | https://support.bull.com/ols/product/platforms/bullion/bullsequana-s/dl/pkgf/technical-state-dvd-packages |

## Available Workarounds

No workaround is available.

## Available Mitigations

See CISA's recommendations [6].

## Available Exploits/PoC

IPMI weaknesses are exploited occasionally.

## References

1. https://www.ibm.com/docs/en/power8/8348-21C?topic=ipmi-risks-using-power-systems-openpower-systems
2. https://nvd.nist.gov/vuln/detail/CVE-2013-4037
3. https://nvd.nist.gov/vuln/detail/CVE-2013-4786
4. https://exchange.xforce.ibmcloud.com/vulnerabilities/86173
5. http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5093463
6. https://www.cisa.gov/news-events/alerts/2013/07/26/risks-using-intelligent-platform-management-interface-ipmi

## 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.