EVIDEN
an atos business

Security Bulletin

Vulnerability in Hashicorp Vault and Vault Enterprise

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1298**
Created	:	**24 May 2024**
Version	:	**0.3**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**2 September 2024**
Keywords	:	**CVE-2024-2048**

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	2024/05/23	Initial Eviden template
0.2	2024/09/02	Table with affected products updated. Removing SMCxscale 2.x as it will be released later, incorporating a fixed version, and therefore not affected.
0.3	2024/09/02	TLP changed for CLEAR

Executive summary

Vault and Vault Enterprise ("Vault") TLS certificate auth method did not correctly validate client certificates when configured with a non-CA certificate as trusted certificate. In this configuration, an attacker may be able to craft a malicious certificate that could be used to bypass authentication. Fixed in Vault 1.15.5 and 1.14.10.

SMC xScale, while using Vault, is not affected.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-2048	8.1	Improper Certificate Validation

Vault offers a wide range of auth methods 16 for authentication, including TLS client certificates 9. Vault's TLS auth method supports trusted certificates signed by certificate authorities as well as non-CA signed certificates.

Vault relies on Golang's TLS libraries to validate client certificates, in combination with further checks in Vault's code. It was discovered that in the case of non-CA signed trusted certificates, Vault insufficiently validated this certificate. As a result, this attacker could use a maliciously crafted certificate to bypass authentication, should the attacker have out-of-band access to information about this public trusted certificate.

Affected products

Products	Fixed version	Status	Comments
SMC xScale 1.x	-	Not affected	Usage of Vault is done through password and not TLS certificate.

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

Customers using the TLS auth method with a non-CA certificate as a trusted certificate in their Vault installation should evaluate the risk associated with this issue and consider upgrading to Vault Enterprise 1.15.5, 1.14.10, or newer. Please refer to Upgrading Vault for general guidance and version-specific upgrade notes.

Eviden informs that xScale is not affected. The usage of Vault is done through password and not TLS certificate.

Available Vendor Patches

This vulnerability is fixed in Vault 1.15.5 and 1.14.10.

Available Workarounds

No workaround is available.

Available Mitigations

No mitigation identified.

Available Exploits/PoC

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

References

1. https://nvd.nist.gov/vuln/detail/CVE-2024-2048
2. https://discuss.hashicorp.com/t/hcsec-2024-05-vault-cert-auth-method-did-not-correctly-validate-non-ca-certificates/63382
3. https://securityonline.info/cve-2024-2048-hashicorps-vault-vulnerability-puts-secrets-at-risk/
4. https://developer.hashicorp.com/vault/tutorials/standard-procedures/sop-upgrade?in=vault%2Fstandard-procedures

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 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.