EVIDEN
an atos business

Security Bulletin

RCE Vulnerability in Shim

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1083**
Created	:	**22 March 2024**
Version	:	**0.3**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**3 May 2024**
Keywords	:	**CVE-2023-40547**

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	2024/02/27	Initial Neutralization version
0.2	2024/03/22	TLP changed for CLEAR
0.3	2024/05/03	Closing the case

Executive summary

On the 2nd of February, 2024, information regarding a recently identified vulnerability, known as CVE-2023-40547, was made public. This vulnerability affects the shim software, which plays a crucial role in the boot process of numerous Linux distributions by facilitating Secure Boot. The discovery and reporting of this vulnerability were credited to Bill Demirkapi from Microsoft's Security Response Center. The specific vulnerability arises from the mishandling of the HTTP protocol, resulting in an out-of-bounds write that has the potential to compromise the entire system.

There are several attack possibilities that could be used to exploit this vulnerability. A potential threat actor has the capability to execute a Man-in-the-Middle (MiTM) attack, thereby intercepting the HTTP traffic exchanged between the target and the HTTP server responsible for delivering files to facilitate HTTP boot. This attacker can position themselves on any network segment situated between the target and the authorized server.

The vulnerability can also be exploited locally by an attacker with enough privileges to manipulate data in the EFI Variables or on the EFI partition. This can be accomplished with a live Linux USB stick. The boot order can then be changed such that a remote and vulnerable shim is loaded on the system. This shim is then used to execute privileged code from the same remote server, all without ever disabling Secure Boot. A potential threat actor who shares the same network as the target has the ability to exploit PXE in order to chain-load a susceptible shim bootloader.

The system can be compromised by an attacker who exploits this vulnerability, enabling them to assume control even before the kernel is loaded. Consequently, they acquire privileged access and possess the capability to bypass any controls established by the kernel and operating system.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-40547	8.3	CWE-787 Out-of-bounds Write CWE-346 Origin Validation Error

		AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

CVE-2023-40547 – score 8.3

A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. This flaw is only exploitable during the early boot phase, an attacker needs to perform a Man-in-the-Middle or compromise the boot server to be able to exploit this vulnerability successfully.

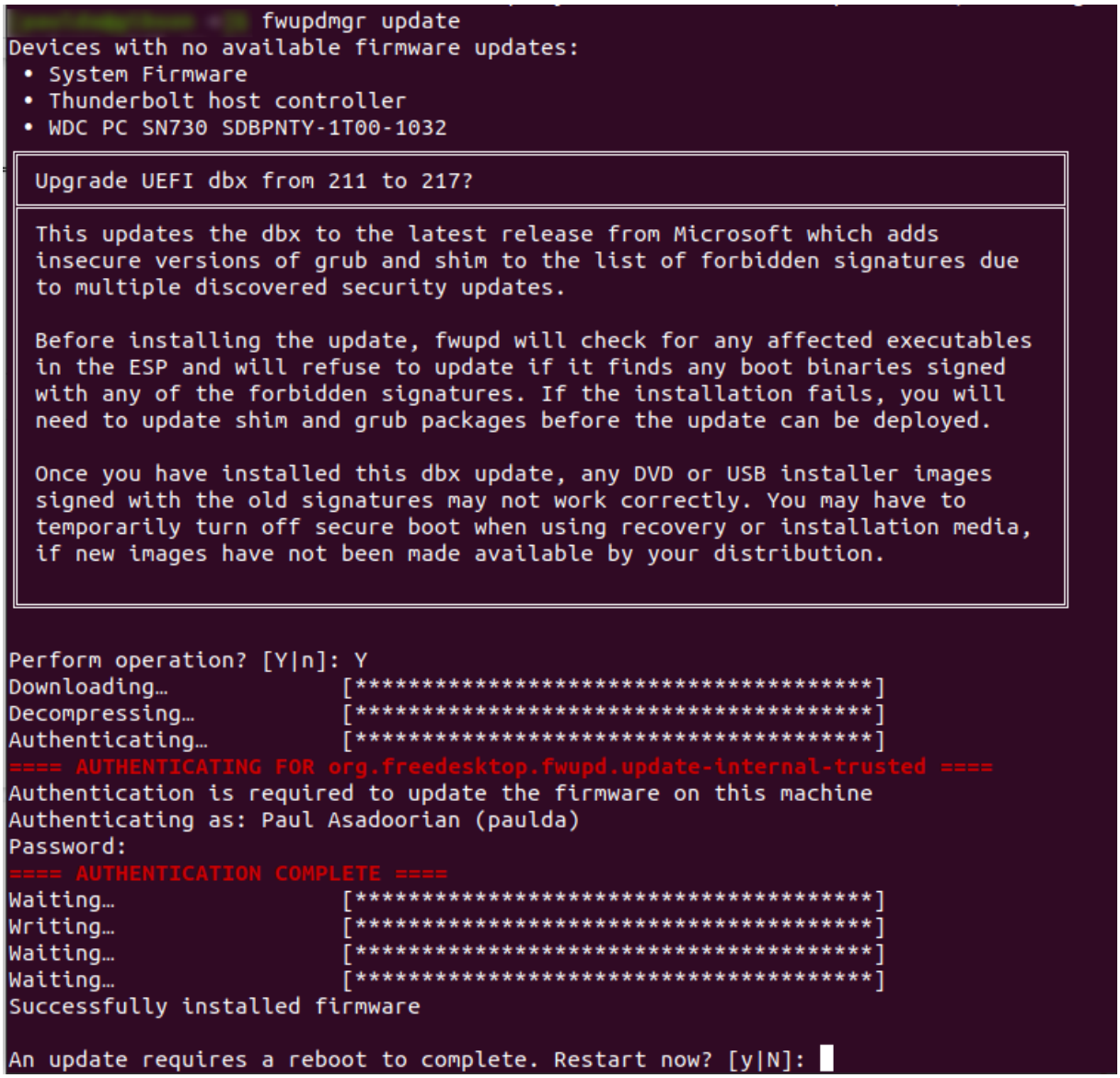
Affected products

Shim package is installed in our platform but not used.

The update of the Secure Boot chain of trust is imperative. It entails the necessity to update the UEFI Secure Boot DBX, which is the revocation list, by incorporating the hashes of the susceptible shim software. Furthermore, measures need to be implemented to ensure the signing of new patched versions of shim using the Microsoft 3rd Party CA.

It is crucial to perform this task concurrently with the update to the latest shim version that includes the patch. The sequence of actions holds significance, as users need to initially update to the most recent shim version and subsequently apply the DBX update.

One of the best ways to apply a DBX update on Linux systems is to use fwupd. This can be done from the command line, provided fwupd is installed, by issuing the ‘fwupdmgr update’ command, as shown below:



Available Vendor Patches

No validated patch is available at the time. Eviden is working with its suppliers to distribute updates as soon as possible.

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

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

Bull Sequana E	https://support.bull.com/ols/product/platforms/bullion/bullsequana-edge-servers/dl/pkgf/pkgf
Bull Sequana X1000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x1000/dl/pkgf/pkg
Bull Sequana XH2000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh2000/dl/pkgf/pkg
Bull Sequana X400-E5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkg
Bull Sequana X400-A5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400-a5/dl/pkgf/pkg
Bull Sequana X800 / QLM	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x800/dl/pkgf/pkg

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. http://www.openwall.com/lists/oss-security/2024/01/26/1
2. https://access.redhat.com/security/cve/CVE-2023-40547
3. https://bugzilla.redhat.com/show_bug.cgi?id=2234589
4. https://nvd.nist.gov/vuln/detail/CVE-2023-40547

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.