Executive Report

External Vulnerability Assessment

Produced by IsaiX Cyber Services
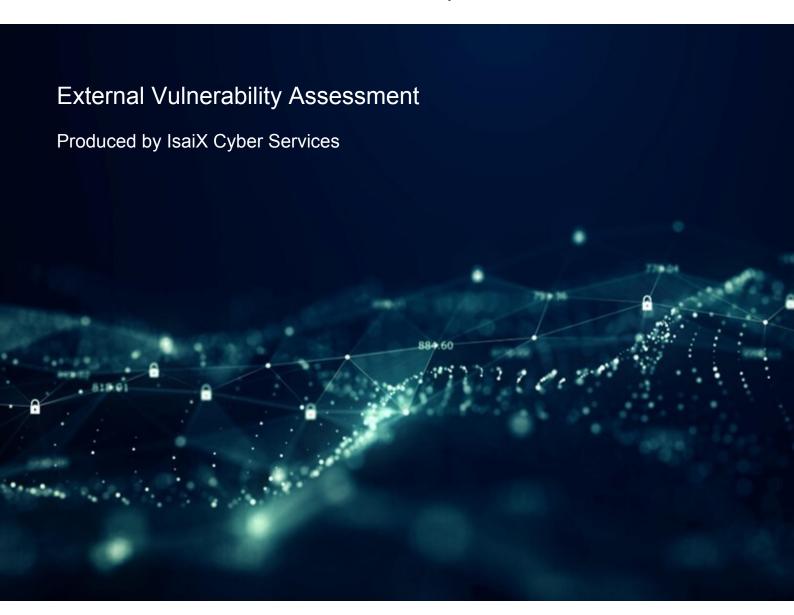
Presented to:

IsaiX Technologies Inc.
Coach 5
417-4030 Rue St-Ambroise Montreal, QC H4C2C7

LOGO

Scan Date: Mar 14 2024

ISAIX

1. Introduction

1.1 Purpose

Welcome to the IsaiX Cyber Level 1 vulnerability scan report generated through our web-hosted portal and automated scanning tools at https://scanner.isaix.com/. The purpose of this report is twofold:

1. For business leaders: to provide an understanding of the technical vulnerabilities of your web assets and offer a new line of sight to support the governance of your cyber resilience and assess your cyber business risk.

2. For IT support resources: to provide detailed insights into the vulnerabilities of your web assets and the references for the remediation of the vulnerabilities.

1.2 Managing your Cyber Risk

In today's threat landscape, cyber criminals are developing new vulnerabilities daily to attack your infrastructure and exploit your business. Exploitation of any vulnerability in your cyber security may create financial, operational and legal exposure and risks. Some of these risks include:

- Theft or loss of information through unauthorized and malicious access

- Disruption of service caused by compromised systems

- Reputation damage resulting from leaks or a loss of control and mis-direction of your web assets

- Ransom or blackmail resulting from theft

- Physical threats to property or personnel through intrusion and control of equipment

- Regulatory breaches and fines

To assess the business risk associated with a particular vulnerability, the vulnerability must beviewed in the context of the system in which it is found, the likelihood that the vulnerability could be used by malicious actors and the potential impact to the business if it were exploited.

Routine, 3rd party assessment of your vulnerabilities and diligent ongoing maintenance of your cyber security systems and the regular training of employees and partners are essential functions of governance.

1.3 The Vulnerability Scan

This Level 1 assessment was conducted by an automated service that uses a number of commonly recognized open-source cyber security tools and proprietary scans to simulate attacks or

exploitations on the target IP addresses assessed by the company.

1.4 Testing Scope

IsaiX Cyber processed target IP addresses entered through its platform. These were:

IPs / Domains / Hosts :

IP Address	Domain Name
52.228.63.192	coach5.isxapps.com

1.5 Disclaimer of Liability and Limitation of the Scan

While IsaiX Cyber can discover numerous threat vectors, no system can guarantee the identification of all possible threats. IsaiX Cyber offers no warranties, representations or legal certifications concerning the applications or systems it scans. Nothing in this document is intended to represent or warrant that security testing was complete and without error, nor does this document represent or warrant that the application or systems it scans are suitable to the task, free of other defects than reported, or compliant with any industry standards.

This report cannot and does not protect against personal or business loss as the result of use of the applications or systems described.

This report contains information on the systems and/or web applications that existed as of Mar 14 2024.

IsaiX Cyber's scanning is a "point in time", level 1 assessment of external web address (es) only and as such it is possible that vulnerabilities not found by the IsaiX scan exists on:

    a) Internal networks;

    b) VOIP or mobile applications;

    c) Operating equipment;

which have not been scanned by our system or that the configuration of the web assets in the environment could have changed, or that new threats have emerged since the IsaiX scan was conducted.

1.6 Distribution of this Report

ISAIX

IsaiX recommends that this report be maintained and circulated in a secure environment only. By accepting delivery of this report, the company holds IsaiX harmless of any damages resulting from its distribution.The offers no guarantees that this PDF file has not been edited by the receiving party to include or omit any information not present on the original output of this Executive Report.

2. Summary

2.1 Executive Summary

This report presents the results of the external reconnaissance and vulnerability detection conducted by IsaiX. This scan was conducted using non-credentialed access via a black-box testing approach which scans your external-facing assets (ex. web applications, web services, company websites) to reveal vulnerabilities and web server misconfigurations. These assets are most susceptible to attack and their vulnerabilities are frequently the most exploited.

This vulnerability assessment may have identified flaws that your company should address diligently in order to prevent their exploitation, in consideration of the nature, severity and context of the risk associated with each vulnerability. The details of the vulnerabilities identified, their severity is presented in this document and references to two cyber security industry standard database resources, the Common Vulnerabilities and Exposures (CVE) and the Common Weakness Enumeration (CWE), are provided for further details.

2.2 Risk Profile

Vulnerabilities identified by the scan are grouped and classified for each target as critical, high, medium, low, and informative. The higher the vulnerability is rated, the greater the likelihood that this vulnerability could be exploited as avenues of attack resulting in, for example only, unauthorized access, data breaches, deletions and theft or system system disruption.

The number, type and severity of the identified vulnerabilities, identified in this report may reveal how well your systems are being maintained. To assess the overall risk to your business operations you must consider the context of the vulnerability, value of the asset that could be compromised, the type of data that could be lost or stolen, against the impact of a breach.

The bar graph breakdown of the vulnerabilities are as follows:

ISAIX

Vulnerabilities Found

3. Risk Evaluation

Two well-known industry standard classification systems were applied to assess the severity of vulnerabilities. These were: Common Vulnerability Scoring System (CVSS) versions 3.0 and 2.0. CVSS assigns severity scores to facilitate the prioritization of action plans according to the threat. Scores are calculated based on a formula that depends on several metrics that approximate ease and impact of an exploit. Scores range from 0 to 10, with 10 being the most severe.

Severity	CVSS v3.0	CVSS v2.0	Definition
Critical	9.0-10.0	Not supporting	The presence of a flaw is confirmed and is currently exploited or easily exploited by attackers on the Internet. Without immediate attention, the reputation and operations of the company will be compromised.
High	7.0-8.9	7.0-10.0	The presence of a fault is confirmed. Exploitation of this vulnerability does not require very high technical and / or material capacities.
Medium	4.0-6.9	4.0-6.9	The presence of a fault is to be confirmed. The configuration is not optimal and should be improved, however, this has no immediate impact on the security of the system. More difficult vulnerabilities to exploit that can lead to a denial of service and possibly loss of confidentiality
Low	0.1-3.9	0.0-3.9	The presence of a fault could not be determined with certainty, however, there are several signs that the system is vulnerable, and that further exploration is needed to confirm the existence of this flaw. These vulnerabilities can lead to loss of confidentiality

ISAIX

4. Summary of Findings

In this section, the results of the external scans are represented.

4.1 Major Vulnerabilities List

Vulnerability	System	Risk Level	No. of Instances	Alert Detection Tool
Server Leaks Information via "X-Powered-By" HTTP Response Header Field	ISAIX	High	1	curl
Missing Anti-clickjacking Header	ISAIX	Medium	1	nikto
Content Security Policy (CSP) Header Not Set	ISAIX	Medium	3	spider owasp
X-Content-Type-Options Header Missing	ISAIX	Medium	1	curl
Retrieved x-powered-by header: ASP.NET.	ISAIX	Medium	1	nikto with report
Retrieved x-aspnet-version header: 2.0.50727.	ISAIX	Medium	1	nikto with report
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.	ISAIX	Medium	1	nikto with report
X-AspNet-Version Response Header	ISAIX	Medium	1	nikto
X-Content-Type-Options Header Missing	ISAIX	Low	2	spider owasp
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	ISAIX	Low	4	spider owasp
TLS 1.2 Weak Protocol	ISAIX	Informational	1	sslyze
This might be interesting.	ISAIX	Informational	1	nikto with report
The anti-clickjacking X-Frame-Options header is not present.	ISAIX	Informational	1	nikto with report
Cyber PORT Scanner 80/tcp	ISAIX	Informational	1	nmap-vuln
Cyber PORT Scanner 443/tcp	ISAIX	Informational	1	nmap-vuln
Cyber PORT Scanner 8080/tcp	ISAIX	Informational	1	nmap-vuln
Cyber PORT Scanner 8443/tcp	ISAIX	Informational	1	nmap-vuln

5. Scan Overview

This section represents the Number of Occurrences for each identified vulnerability per IP / Host along with their risk level. Please note that the Number of Occurrence increases if the same vulnerability is found on another website on the same IP/Host:

Host: 52.228.63.192

0	1	8	2	7
Critical	High	Medium	Low	Info

6. Detailed Vulnerability Analysis

6.1 Server Leaks Information via "X-Powered-By" HTTP Response Header Field

Risk Factor: High	Occurrences: 1

Description: A CWE-200: Information Exposure vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause the disclosure of SNMP information when reading memory blocks from the controller over Modbus.

Solution: N/A

CVSS 3: 7.5

CVSS 2: 5.0

Tool: curl

CWE: CWE-200

Evidence:

```
X-Powered-By
```

6.2 Missing Anti-clickjacking Header

Risk Factor: Medium	Occurrences: 1

Description: The X-Frame-Options headers were applied inconsistently on some HTTP responses, resulting in duplicate or missing security headers. Some browsers would interpret these results incorrectly, allowing clickjacking attacks. Mitigation: The fix to consistently apply the security headers was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.

Solution: N/A

CVSS 3: 6.5

CVSS 2: 4.3

Tool: nikto

CWE: CWE-1021

Evidence:

The anti-clickjacking X-Frame-Options header is not present.

6.3 Content Security Policy (CSP) Header Not Set

Risk Factor: Medium	Occurrences: 3

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

CVSS 3: N/A

CVSS 2: N/A

Tool: spider owasp

CWE: CWE-693

Evidence:

N/A

6.4 X-Content-Type-Options Header Missing

Risk Factor: Medium	Occurrences: 1

Description: For ABB eSOMS versions 4.0 to 6.0.3, the X-Content-Type-Options Header is missing in the HTTP response, potentially causing the response body to be interpreted and displayed as different content type other than declared. A possible attack scenario would be unauthorized code execution via text interpreted as JavaScript.

Solution: N/A

CVSS 3: 6.1

CVSS 2: 4.3

Tool: curl

CWE: CWE-436,CWE-94,CWE-16

Evidence:

X-Content-Type-Options: nosniff

6.5 Retrieved x-powered-by header: ASP.NET.

Risk Factor: Medium	Occurrences: 1

Description: Label Studio, an open source data labeling tool had a remote import feature allowed users to import data from a remote web source, that was downloaded and could be viewed on the website. Prior to version 1.10.1, this feature could had been abused to download a HTML file that executed malicious JavaScript code in the context of the Label Studio website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. `data_import/uploader.py` lines 125C5 through 146 showed that if a URL passed the server side request forgery verification checks, the contents of the file would be downloaded using the filename in the URL. The downloaded file path could then be retrieved by sending a request to `/api/projects/{project_id}/file-uploads?ids=[{download_id}]` where `{project_id}` was the ID of the project and `{download_id}` was the ID of the downloaded file. Once the downloaded file path was retrieved by the previous API endpoint, `data_import/api.py`lines 595C1 through 616C62 demonstrated that the `Content-Type` of the response was determined by the file extension, since `mimetypes.guess_type` guesses the `Content-Type` based on the file extension. Since the `Content-Type` was determined by the file extension of the downloaded file, an attacker could import in a `.html` file that would execute JavaScript when visited. Version 1.10.1 contains a patch for this issue. Other remediation strategies are also available. For all user provided files that are downloaded by Label Studio, set the `Content-Security-Policy: sandbox;` response header when viewed on the site. The `sandbox` directive restricts a page's actions to prevent popups, execution of plugins and scripts and enforces a `same-origin` policy. Alternatively, restrict the allowed file extensions that may be downloaded.

Solution: N/A

CVSS 3: 6.1

CVSS 2: N/A

Tool: nikto with report

CWE: CWE-79,CWE-79

Evidence:

```
/
```

6.6 Retrieved x-aspnet-version header: 2.0.50727.

Risk Factor: Medium	Occurrences: 1

Description: Label Studio, an open source data labeling tool had a remote import feature allowed users to import data from a remote web source, that was downloaded and could be viewed on the website. Prior to version 1.10.1, this feature could had been abused to download a HTML file that executed malicious JavaScript code in the context of the Label Studio website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. `data_import/uploader.py` lines 125C5 through 146 showed that if a URL passed the server side request forgery verification checks, the contents of the file would be downloaded using the filename in the URL. The downloaded file path could then be retrieved by sending a request to `/api/projects/{project_id}/file-uploads?ids=[{download_id}]` where `{project_id}` was the ID of the project and `{download_id}` was the ID of the downloaded file. Once the downloaded file path was retrieved by the previous API endpoint, `data_import/api.py`lines 595C1 through 616C62 demonstrated that the `Content-Type` of the response was determined by the file extension, since `mimetypes.guess_type` guesses the `Content-Type` based on the file extension. Since the `Content-Type` was determined by the file extension of the downloaded file, an attacker could import in a `.html` file that would execute JavaScript when visited. Version 1.10.1 contains a patch for this issue. Other remediation strategies are also available. For all user provided files that are downloaded by Label Studio, set the `Content-Security-Policy: sandbox;` response header when viewed on the site. The `sandbox` directive restricts a page's actions to prevent popups, execution of plugins and scripts and enforces a `same-origin` policy. Alternatively, restrict the allowed file extensions that may be downloaded.

Solution: N/A

CVSS 3: 6.1

CVSS 2: N/A

Tool: nikto with report

CWE: CWE-79,CWE-79

Evidence:

/Z280VYJZ.aspx

6.7 The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

Risk Factor: Medium	Occurrences: 1

Description: Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 affects all Kirby sites that might have potential attackers in the group of authenticated Panel users or that allow external visitors to upload an arbitrary file to the content folder. Kirby sites are not affected if they don't allow file uploads for untrusted users or visitors or if the file extensions of uploaded files are limited to a fixed safe list. The attack requires user interaction by another user or visitor and cannot be automated. An editor with write access to the Kirby Panel could upload a file with an unknown file extension like `.xyz` that contains HTML code including harmful content like `<script></script>`

Solution: N/A

CVSS 3: 5.4

CVSS 2: N/A

Tool: nikto with report

CWE: CWE-79

Evidence:

/

6.8 X-AspNet-Version Response Header

Risk Factor: Medium	Occurrences: 1

Description: Microsoft .NET Framework 1.1 SP1, 2.0 SP1 and SP2, 3.5, 3.5 SP1, 3.5.1, and 4.0, as used for ASP.NET in Microsoft Internet Information Services (IIS), provides detailed error codes during decryption attempts, which allows remote attackers to decrypt and modify encrypted View State (aka __VIEWSTATE) form data, and possibly forge cookies or read application files, via a padding oracle attack, aka "ASP.NET Padding Oracle Vulnerability."

Solution: N/A

CVSS 3: N/A

CVSS 2: 6.4

Tool: nikto

CWE: CWE-209

Evidence:

Retrieved x-aspnet-version header: 2.0.50727

6.9 X-Content-Type-Options Header Missing

Risk Factor: Low   **Occurrences: 2**

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

CVSS 3: N/A

CVSS 2: N/A

Tool: spider owasp

CWE: CWE-693

Evidence:

N/A

6.10 Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Risk Factor: Low	Occurrences: 4

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

CVSS 3: N/A

CVSS 2: N/A

Tool: spider owasp

CWE: CWE-200

Evidence:

> X-Powered-By: ASP.NET

6.11 TLS 1.2 Weak Protocol

Risk Factor: Informational	Occurrences: 1

Description: The remote service accepts connections encrypted using TLS 1.2.

Solution: N/A

CVSS 3: N/A

CVSS 2: N/A

Tool: sslyze

CWE: N/A

Evidence:

```
Attempted            to        connect        using        156        cipher        suites.
                The   server   accepted   the   following   6   cipher   suites:
        TLS_RSA_WITH_AES_256_GCM_SHA384                256
        TLS_RSA_WITH_AES_256_CBC_SHA256                256
        TLS_RSA_WITH_AES_256_CBC_SHA                   256
        TLS_RSA_WITH_AES_128_GCM_SHA256                128
        TLS_RSA_WITH_AES_128_CBC_SHA256                128
        TLS_RSA_WITH_AES_128_CBC_SHA                   128
    The  group  of  cipher  suites  supported  by  the  server  has  the  following  properties:
        Forward   Secrecy                           INSECURE  -  Not  Supported
    Legacy RC4 Algorithm            OK - Not Supported
```

6.12 This might be interesting.

Risk Factor: Informational	Occurrences: 1

Description: In the Linux kernel, the following vulnerability has been resolved: llc: call sock_orphan() at release time syzbot reported an interesting trace [1] caused by a stale sk->sk_wq pointer in a closed llc socket. In commit ff7b11aa481f ("net: socket: set sock->sk to NULL after calling proto_ops::release()") Eric Biggers hinted that some protocols are missing a sock_orphan(), we need to perform a full audit. In net-next, I plan to clear sock->sk from sock_orphan() and amend Eric patch to add a warning. [1] BUG: KASAN: slab-use-after-free in list_empty include/linux/list.h:373 [inline] BUG: KASAN: slab-use-after-free in waitqueue_active include/linux/wait.h:127 [inline] BUG: KASAN: slab-use-after-free in sock_def_write_space_wfree net/core/sock.c:3384 [inline] BUG: KASAN: slab-use-after-free in sock_wfree+0x9a8/0x9d0 net/core/sock.c:2468 Read of size 8 at addr ffff88802f4fc880 by task ksoftirqd/1/27 CPU: 1 PID: 27 Comm: ksoftirqd/1 Not tainted 6.8.0-rc1-syzkaller-00049-g6098d87eaf31 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 Call Trace: <task> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x1b0 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc4/0x620 mm/kasan/report.c:488 kasan_report+0xda/0x110 mm/kasan/report.c:601 list_empty include/linux/list.h:373 [inline] waitqueue_active include/linux/wait.h:127 [inline] sock_def_write_space_wfree net/core/sock.c:3384 [inline] sock_wfree+0x9a8/0x9d0 net/core/sock.c:2468 skb_release_head_state+0xa3/0x2b0 net/core/skbuff.c:1080 skb_release_all net/core/skbuff.c:1092 [inline] napi_consume_skb+0x119/0x2b0 net/core/skbuff.c:1404 e1000_unmap_and_free_tx_resource+0x144/0x200 drivers/net/ethernet/intel/e1000/e1000_main.c:1970 e1000_clean_tx_irq drivers/net/ethernet/intel/e1000/e1000_main.c:3860 [inline] e1000_clean+0x4a1/0x26e0 drivers/net/ethernet/intel/e1000/e1000_main.c:3801 __napi_poll.constprop.0+0xb4/0x540 net/core/dev.c:6576 napi_poll net/core/dev.c:6645 [inline] net_rx_action+0x956/0xe90 net/core/dev.c:6778 __do_softirq+0x21a/0x8de kernel/softirq.c:553 run_ksoftirqd kernel/softirq.c:921 [inline] run_ksoftirqd+0x31/0x60 kernel/softirq.c:913 smpboot_thread_fn+0x660/0xa10 kernel/smpboot.c:164 kthread+0x2c6/0x3a0 kernel/kthread.c:388 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/entry/entry_64.S:242 </task> Allocated by task 5167: kasan_save_stack+0x33/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:314 [inline] __kasan_slab_alloc+0x81/0x90 mm/kasan/common.c:340 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3813 [inline] slab_alloc_node mm/slub.c:3860 [inline] kmem_cache_alloc_lru+0x142/0x6f0 mm/slub.c:3879 alloc_inode_sb include/linux/fs.h:3019 [inline] sock_alloc_inode+0x25/0x1c0 net/socket.c:308 alloc_inode+0x5d/0x220 fs/inode.c:260 new_inode_pseudo+0x16/0x80 fs/inode.c:1005 sock_alloc+0x40/0x270 net/socket.c:634 __sock_create+0xbc/0x800 net/socket.c:1535 sock_create net/socket.c:1622 [inline] __sys_socket_create net/socket.c:1659 [inline] __sys_socket+0x14c/0x260 net/socket.c:1706 __do_sys_socket net/socket.c:1720 [inline] __se_sys_socket net/socket.c:1718 [inline] __x64_sys_socket+0x72/0xb0 net/socket.c:1718 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xd3/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Freed by task 0: kasan_save_stack+0x33/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 kasan_save_free_info+0x3f/0x60 mm/kasan/generic.c:640 poison_slab_object mm/kasan/common.c:241 [inline] __kasan_slab_free+0x121/0x1b0 mm/kasan/common.c:257 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2121 [inlin ---truncated---

---

Solution: N/A

CVSS 3: N/A

CVSS 2: N/A

Tool: nikto with report

CWE:

Evidence:

/test.html

6.13 The anti-clickjacking X-Frame-Options header is not present.

Risk Factor: Informational	Occurrences: 1

Description: In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Check mailbox/SMT channel for consistency On reception of a completion interrupt the shared memory area is accessed to retrieve the message header at first and then, if the message sequence number identifies a transaction which is still pending, the related payload is fetched too. When an SCMI command times out the channel ownership remains with the platform until eventually a late reply is received and, as a consequence, any further transmission attempt remains pending, waiting for the channel to be relinquished by the platform. Once that late reply is received the channel ownership is given back to the agent and any pending request is then allowed to proceed and overwrite the SMT area of the just delivered late reply; then the wait for the reply to the new request starts. It has been observed that the spurious IRQ related to the late reply can be wrongly associated with the freshly enqueued request: when that happens the SCMI stack in-flight lookup procedure is fooled by the fact that the message header now present in the SMT area is related to the new pending transaction, even though the real reply has still to arrive. This race-condition on the A2P channel can be detected by looking at the channel status bits: a genuine reply from the platform will have set the channel free bit before triggering the completion IRQ. Add a consistency check to validate such condition in the A2P ISR.

Solution: N/A

CVSS 3: N/A

CVSS 2: N/A

Tool: nikto with report

CWE:

Evidence:

/

6.14 Cyber PORT Scanner 80/tcp

Risk Factor: Informational	Occurrences: 1

Description: A Cyber port scanner is this plugin's function to find out open ports.Cyber port scanner are less intrusive than TCP (full connect) scans against broken services, but if the network is busy, they may cause issues for less capable firewalls and leave open connections on the remote target.

Solution: Use an IP filter to shield your target.

CVSS 3: N/A

CVSS 2: N/A

Tool: nmap-vuln

CWE: N/A

Evidence:

80/tcp open http

6.15 Cyber PORT Scanner 443/tcp

Risk Factor: Informational	Occurrences: 1

Description: A Cyber port scanner is this plugin's function to find out open ports.Cyber port scanner are less intrusive than TCP (full connect) scans against broken services, but if the network is busy, they may cause issues for less capable firewalls and leave open connections on the remote target.

Solution: Use an IP filter to shield your target.

CVSS 3: N/A

CVSS 2: N/A

Tool: nmap-vuln

CWE: N/A

Evidence:

443/tcp open ssl/http

6.16 Cyber PORT Scanner 8080/tcp

Risk Factor: Informational	Occurrences: 1

Description: A Cyber port scanner is this plugin's function to find out open ports.Cyber port scanner are less intrusive than TCP (full connect) scans against broken services, but if the network is busy, they may cause issues for less capable firewalls and leave open connections on the remote target.

Solution: Use an IP filter to shield your target.

CVSS 3: N/A

CVSS 2: N/A

Tool: nmap-vuln

CWE: N/A

Evidence:

> 8080/tcp open http

ISAIX

6.17 Cyber PORT Scanner 8443/tcp

Risk Factor: Informational	Occurrences: 1

Description: A Cyber port scanner is this plugin's function to find out open ports.Cyber port scanner are less intrusive than TCP (full connect) scans against broken services, but if the network is busy, they may cause issues for less capable firewalls and leave open connections on the remote target.

Solution: Use an IP filter to shield your target.

CVSS 3: N/A

CVSS 2: N/A

Tool: nmap-vuln

CWE: N/A

Evidence:

8443/tcp open ssl/http