APPLICATION NOTE

IoT Firmware Security Analysis

Enabling supply chain security and regulatory compliance

KEYSIGHT

Table of Contents

Introduction

Firmware is software that controls the essential functions of IoT devices and is crucial for their operation, however it presents unique security challenges. Typically host security agents are installed to protect and monitor desktop operating systems and applications. However, this approach is not always feasible for protecting device firmware due to the absence of necessary interfaces and constrained hardware resources, often making it invisible to network-based security tools. This security blind spot makes it more difficult to detect firmware vulnerabilities and, consequently, more challenging to address.

Traditional approaches to IoT security assessments typically focus on network and application vulnerabilities, leaving the firmware relatively unchecked. This oversight can lead to significant security risks as attackers can exploit firmware vulnerabilities to gain unauthorized access or control over devices. Given the critical role of firmware, a dedicated approach to firmware analysis is necessary.

Keysight's automated IoT firmware security analysis solution — part of the Keysight IoT Security Assessment product — addresses this gap. This document describes its key features and benefits and includes a step-by-step guide on using the product to conduct IoT firmware security assessments. It serves as a guide for developers, security analysts, and business decision-makers who need to enhance the security of their IoT devices.

Problem Statement

Firmware is fundamental to the operation and security of IoT devices however its opaque nature obscures the software composition and makes securing IoT devices challenging.

For manufacturers and security labs, this complexity presents a multifaceted challenge, they are responsible for ensuring that products are secure and can withstand evolving cyber threats over their lifecycle. The task is daunting and requires a detailed understanding of a diverse range of different IoT device firmware, including any third-party components it might incorporate.

They have a variety of firmware file systems and compression methods that demand specific tools and expertise for practical vulnerability assessment and mitigation.

Manufacturers must also work through complex IoT regulatory standards and frameworks such as NISTIR 8259 and ETSI EN 303 645. Standards evolve in response to emerging threats and technological advancements, so manufacturers must continually adapt their security measures to ensure compliance.

In addition, vulnerabilities can appear at any stage of a device's operational life due to the dynamic nature of cyber threats. This requires ongoing vigilance from manufacturers and continuous monitoring for new vulnerabilities to maintain the security and integrity of IoT devices, especially those deployed in environments where physical access for updates is limited.

In response to these challenges, an automated firmware security analysis solution is vital for security labs and manufacturers. This solution enables deep analysis of firmware composition, vulnerability detection, proof of compliance with current standards, and facilitation of ongoing security monitoring.

Product Description

Keysight’s IoT Firmware Security Analysis Solution — part of our IoT Security Assessment product — is specifically designed to address the security challenges found within the firmware of IoT devices.

The solution can identify vulnerabilities directly within the device's operating code, including everything from extracting the Software Bill of Materials (SBOM) to uncovering associated vulnerabilities, detecting hard-coded credentials that pose unauthorized access risks, pinpointing configuration flaws, identifying weak or expired cryptographic keys and certificates, and finding vulnerable scripts and binary code. This allows for a more comprehensive and proactive security posture assessment, ensuring vulnerabilities are identified and mitigated before they can be exploited.

It is an essential solution for manufacturers, security labs, and end users who are navigating the complexities of ensuring firmware security across a variety of IoT devices, from consumer electronics to industrial systems.

Detailed feature insights

Software Bill of Materials (SBOM) generation

Keysight’s IoT Security Assessment meticulously generates an SBOM for each piece of firmware it analyzes and can export the SBOM in the structured machine-readable SPDX and CycloneDX formats. The generated SBOM lists all software components within the firmware and identifies any known vulnerabilities. This helps you understand the potential security risks present and offers a clear direction for addressing these issues.

CVE detection connected to NVD database

Central to IoT Security Assessment is the CVE detection feature, which is directly linked to the National Vulnerability Database (NVD). Keysight created a proprietary CVE search algorithm designed to perform a nuanced correlation between components within the firmware and their associated CVEs. This algorithm catches CVEs that other similar tools might miss and reduces false positives. This ensures comprehensive scanning for known vulnerabilities and fortifies the firmware against recognized exploits.

Detection of hard-coded credentials

The IoT Security Assessment solution employs advanced scanning techniques to identify instances where usernames, passwords, or cryptographic keys are embedded directly within the firmware. Identifying these early is essential for preventing unauthorized access.

Configuration flaws analysis

This feature provides a thorough examination of the firmware's operating system configuration settings. It identifies insecure configurations that may potentially expose the device to cyber threats. The analysis delivers results with actionable recommendations for enhancing the security of the device's configuration.

Analysis of cryptographic practices

The Keysight solution assesses the cryptographic practices within the firmware, including the strength and implementation of keys and certificates. This ensures protection against interception or tampering with the device's communications.

Proactive detection of potential 0-Day vulnerabilities

One of the most advanced features of IoT Security Assessment is its ability to search for potential 0-day vulnerabilities within binaries inside firmware. This involves using state-of-the-art techniques to uncover vulnerabilities that have yet to be identified or exploited in the wild, so you can proactively protect devices.

Actionable insights for each weakness

Keysight’s solution generates valuable information for every weakness detected, including the associated security domain, Common Weakness Enumeration (CWE) codes, risk level, technical details, attack conditions, exploitation impact, and mitigation strategies. This equips users with the knowledge needed to address vulnerabilities effectively.

Compatibility and specialized focus

Comprehensive operating system support

IoT Security Assessment is designed with the diversity of the IoT firmware binaries in mind. It supports a wide range of operating systems, including those based on Linux and Android, as well as bare-metal or monolithic firmware utilizing ARM Cortex-M architecture.

Analysis of firmware binaries without symbols

A symbol file maps addresses in a firmware binary file to the corresponding function and variable names as defined in the firmware's source code. Thus, it can significantly ease manual and automated analysis of firmware binaries. However, firmware vendors often do not release symbol files to the public or system integrators. Keysight’s solution can conduct security analysis on ARM Cortex-M firmware binaries without symbol files by automatically identifying standard C libraries across widely used embedded firmware toolchains in the target binary.

Benefits

Enhanced security posture

IoT Security Assessment significantly enhances the security posture of IoT devices by thoroughly analyzing firmware for vulnerabilities and security weaknesses. This helps identify and mitigate security risks early in the device lifecycle and reduces the likelihood of successful cyberattacks.

Supply chain security enhancement

Generating a detailed SBOM and associated CVEs plays a pivotal role in enhancing supply chain security. The Keysight solution provides visibility into the software components, such as third-party applications and libraries embedded within the firmware. With this information, manufacturers can take preemptive actions to secure the supply chain and ensure that each component meets the required security standards.

Streamlined compliance

With semi-automated checks against appropriate provisions of industry standards, manufacturers can more easily ensure their devices comply with necessary security standards. This helps maintain high-security standards and simplifies the process of meeting regulatory requirements.

Informed decision-making

The detailed information provided for each detected weakness—including security domain, CWE codes, risk level, technical details, attack condition, exploitation impact, and mitigation strategies empowers users to make informed decisions about how to address vulnerabilities. As a result, you can prioritize remediation efforts based on the potential impact of each weakness.

Efficiency and cost savings

Automating firmware analysis saves significant time and resources compared to manual methods. IoT Security Assessment enables more efficient use of security teams' time by quickly identifying vulnerabilities and offering actionable insights for mitigation, which leads to cost savings in the long run.

Proactive security measures

The ability to detect potential 0-day vulnerabilities and provide detailed analyses of vulnerabilities and weaknesses allows users to adopt a proactive approach to IoT firmware security. This helps you to enhance the resilience of IoT devices against future threats.

Wide range of device support

Keysight’s solution offers broad applicability across the IoT ecosystem with capabilities tailored for both feature-rich operating systems and bare-metal firmware. It ensures that devices of varying complexity and function can benefit from enhanced security analysis and protection.

Applications and Use Cases

Industry applications

Government and defense IoT applications

In government and defense, where the stakes are exceptionally high, it is critical to secure IoT devices against all cyber threats. Firmware analysis capabilities are essential for identifying vulnerabilities that can compromise national security or operational effectiveness. Providing detailed information on each detected vulnerability and weakness with recommended mitigation actions enables defense contractors and government agencies to fortify their IoT applications against espionage and cyber warfare.

Automotive IoT systems

Integrating IoT technologies into automotive systems has transformed the driving experience by offering features like remote diagnostics and enhanced entertainment systems. However, this also introduces vulnerabilities that can be exploited to gain unauthorized control over vehicle systems. Firmware security analysis helps automotive manufacturers identify and mitigate these risks and ensures the safety and privacy of drivers and passengers. Moreover, maintaining up-to-date security measures is essential for meeting automotive industry standards and protecting against liability issues.

Industrial IoT (IIoT) systems

IoT devices play an important role in monitoring and controlling machinery, supply chains, and operational processes in industrial environments. Their security is paramount, as any breach can lead to significant operational disruptions, financial losses, or even physical danger to personnel. Analyzing the devices' firmware for security vulnerabilities and weaknesses allows manufacturers to ensure that their IIoT devices are robust against cyber-attacks.

Healthcare device security

Medical IoT devices, ranging from wearable health monitors to sophisticated diagnostic equipment, handle highly sensitive patient data and are integral to patient care and medical procedures. The consequences of security breaches in this sector can be dire, including compromising patient confidentiality and manipulating device functionalities. By conducting firmware analyses, medical device manufacturers can detect and rectify vulnerabilities, ensure patient data remains confidential, and that devices operate as intended.

Telecom device security

Securing devices like routers and modems becomes critical as the telecommunications industry integrates more IoT technologies. These devices are vital for global communication, and any vulnerability can lead to significant data breaches. IoT firmware analysis enables manufacturers to detect and fix vulnerabilities early.

Enterprise IoT

The challenge for manufacturers of enterprise IoT devices, such as security cameras, networked printers, and video conferencing systems, is maintaining product security. IoT Security Assessment helps manufacturers by analyzing firmware for vulnerabilities and generating SBOM, which helps them detect security vulnerabilities as soon as CVEs are identified, and devices receive timely security updates.

Consumer electronics

In the consumer electronics sector, where competition is fierce and user experience is paramount, the security of IoT devices like smartwatches and fitness trackers is often a key differentiator. Manufacturers can protect users from data breaches and unauthorized device access by employing the Keysight solution to ensure firmware is free from vulnerabilities. Moreover, providing actionable insights and mitigation strategies helps manufacturers address vulnerabilities efficiently and reduce time-to-market for secure and reliable products.

Smart home devices

For smart home device manufacturers, Keysight’s firmware security analysis solution is essential for identifying and addressing vulnerabilities that can compromise user privacy and home security. Smart home devices, such as thermostats, lighting systems, and security cameras, often interconnect and are remotely accessible, presenting a significant security risk if not properly managed. By using the Keysight solution, manufacturers can maintain the security of these devices and issue timely updates.

Smart city infrastructure

Cities are becoming smarter by integrating IoT technologies for traffic management, public safety, and utility services. IoT firmware analysis enables city planners and technology providers to identify and address vulnerabilities within smart city infrastructure and ensure resilience against cyber-attacks that can disrupt city operations and compromise citizen data.

Specific use cases

Success story: Elevating product security for market access and reputation protection

Background

A manufacturer of enterprise IoT devices faced a strategic decision point: integrate robust security into their product lineup. This necessity was driven by the need to comply with IoT security standards and SBOM generation regulations, which are pivotal for accessing specific markets, including government and critical infrastructure contracts. Recognizing that security is often a significant differentiator against competitors, the manufacturer aimed to leverage it as a competitive advantage to secure large deals.

Challenge

The manufacturer produced a diverse range of over 30 products, each undergoing a firmware update cycle every two months. Given the complexity and the frequency of updates, a detailed cost estimation for ongoing security checks and SBOM generation by a third-party cybersecurity firm was calculated as follows: 6 days per firmware analysis * 6 times a year * $1,000 per day * 30 products, totaling around $1M annually. Beyond the financial aspect, there was an awareness of the potential long-term reputational damage from being highlighted in the news for security vulnerabilities, a situation the manufacturer wanted to avoid at all costs.

Strategic decision

The manufacturer opted to implement the automated IoT firmware security analysis solution—part of the Keysight IoT Security Assessment product — to address these challenges and secure a competitive edge. The solution promised efficiency in conducting thorough security checks, generating SBOMs, and enabling the manufacturer to identify and address new vulnerabilities across all products swiftly.

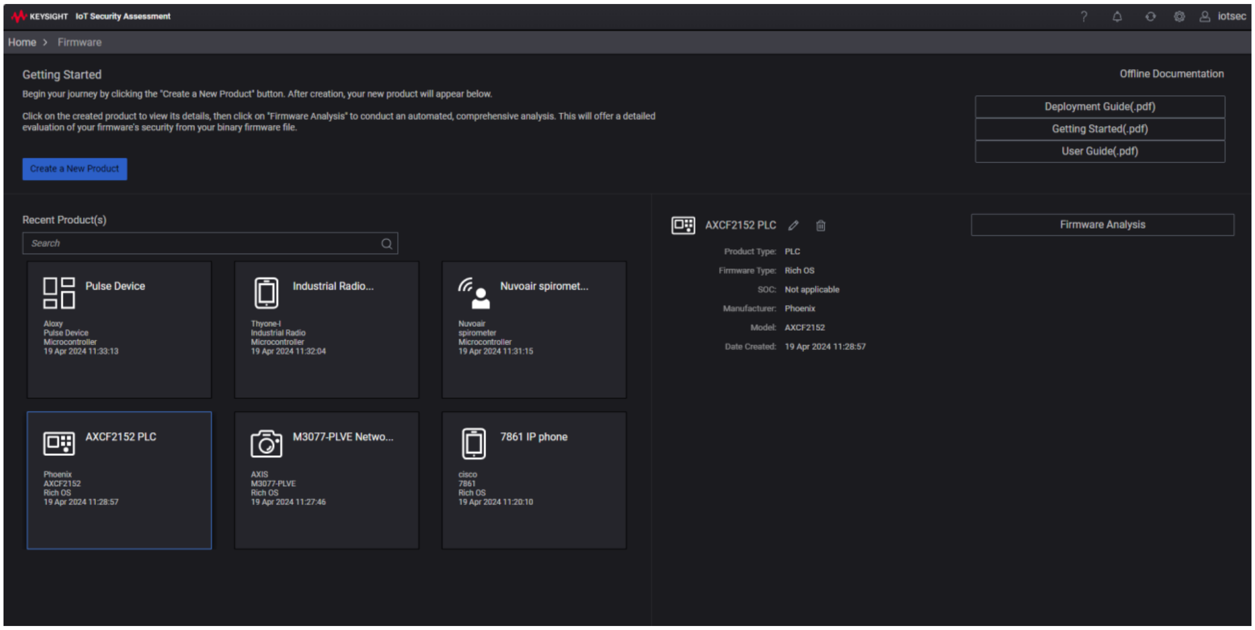
Results

- **Delivered Cost Efficiency:** The solution's adoption drastically reduced the need for expensive third-party assessments, saving the manufacturer close to $1M annually in cybersecurity firm fees.
- **Streamlined Security Analysis:** Adopting the solution cut down the time for security assessments from six days to just minutes for each firmware. This acceleration enabled faster updates and iterations across their product range and reduced errors that can occur with manual analysis, resulting in more reliable and secure firmware deployments.
- **Secured Large Deals:** With enhanced security capabilities, the manufacturer successfully won three multi-million-dollar bids, all of which had strict security requirements. This showcased the direct ROI of their strategic decision and positioned them as a leader in secure IoT device manufacturing.
- **Met U.S. Government Supplier Qualification:** Meeting the compliance requirements for SBOM generation enabled the manufacturer to become a qualified supplier for the U.S. government, marking a significant achievement in credibility and market access.
- **Protected Reputation:** Proactively managing firmware vulnerabilities helped the manufacturer avoid the pitfalls of negative publicity associated with insecure products. This protective measure ensured their brand continued to be known for quality and security, safeguarding their market position and future business prospects.

User Guide

The product page allows you to create a new product. An IoT product is identified by its manufacturer and model. To start, click "Create a New Product," then fill out the product details in the provided form fields. Select the product type, then enter the product name, firmware type, manufacturer, and model.

The firmware type options include "Rich OS" and "Microcontroller." Rich OS firmware is based on complex, feature-rich operating systems like Linux and Android. Microcontroller firmware is directly programmed into the non-volatile memory of microcontrollers. Keysight currently supports the ARM Cortex-M architecture with specialized checks for Nordic and STMicroelectronics SDKs for this type of firmware. You can choose between Generic ARM Cortex-M, Nordic, and STMicro SoCs when selecting microcontroller firmware. If you are unsure of the SoC, select Generic ARM Cortex-M. It is important to select the proper firmware type and SoC at this stage, as it affects the backend engine for analysis. Incorrect selections may lead to no results or improper analysis. Once the information is entered, click the "OK" button to add the product.



Getting Started

Begin your journey by clicking the "Create a New Product" button. After creation, your new product will appear below.

Click on the created product to view its details, then click on "Firmware Analysis" to conduct an automated, comprehensive analysis. This will offer a detailed evaluation of your firmware's security from your binary firmware file.

Pulse Device
Aloxy
Pulse Device
Microcontroller
19 Apr 2024 11:33:13

Industrial Radio...
Thyone-I
Industrial Radio
Microcontroller
19 Apr 2024 11:32:04

Nuvoair spiromet...
Nuvoair
spirometer
Microcontroller
19 Apr 2024 11:31:15

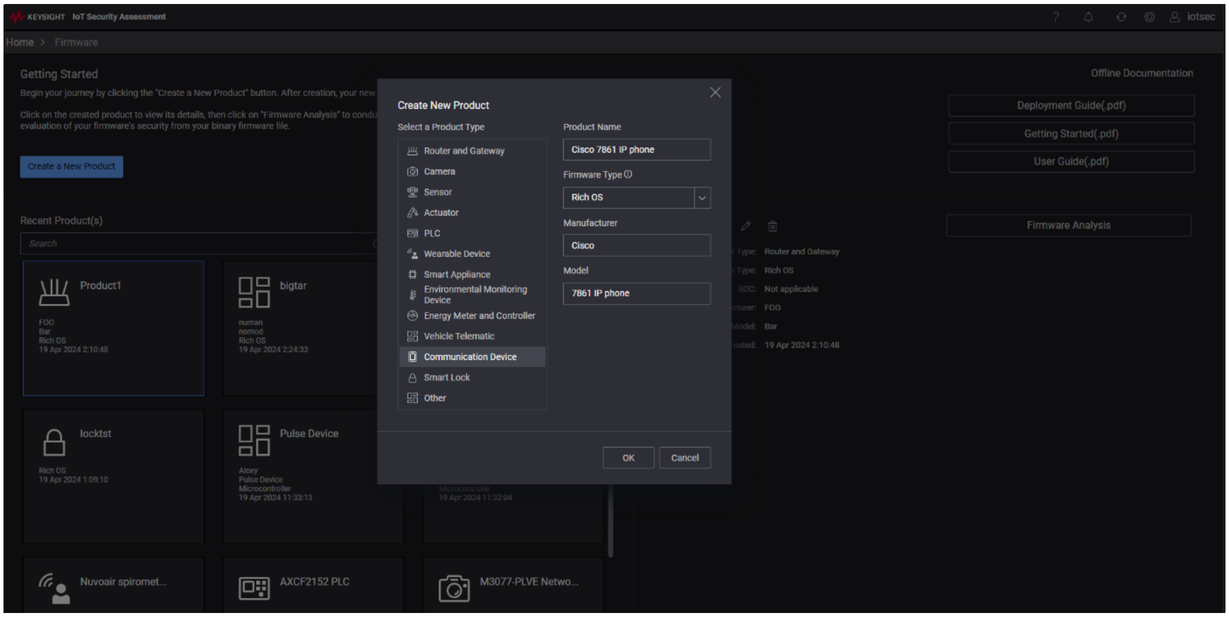
AXCF2152 PLC
Phoenix
AXCF2152
Rich OS
19 Apr 2024 11:28:57

M3077-PLVE Netwo...
AXIS
M3077-PLVE
Rich OS
19 Apr 2024 11:27:46

7861 IP phone
cisco
7861
Rich OS
19 Apr 2024 11:20:10

AXCF2152 PLC

Product Type: PLC
Firmware Type: Rich OS
SOC: Not applicable
Manufacturer: Phoenix
Model: AXCF2152
Date Created: 19 Apr 2024 11:28:57



Getting Started

Begin your journey by clicking the "Create a New Product" button. After creation, your new

Click on the created product to view its details, then click on "Firmware Analysis" to condu
evaluation of your firmware's security from your binary firmware file.

Product1
FOO
Bar
Rich OS
19 Apr 2024 2:10:48

bigtar
numan
nomod
Rich OS
19 Apr 2024 2:24:33

locktst
Rich OS
19 Apr 2024 1:09:10

Pulse Device
Aloxy
Pulse Device
Microcontroller
19 Apr 2024 11:33:13

Microcontroller
19 Apr 2024 11:32:04

Nuvoair spiromet...

AXCF2152 PLC

M3077-PLVE Netwo...

Type: Router and Gateway
Type: Rich OS
SOC: Not applicable
cturer: FOO
Model: Bar
eated: 19 Apr 2024 2:10:48

Create New Product

Select a Product Type: Communication Device

Product Name: Cisco 7861 IP phone

Firmware Type ⓘ: Rich OS

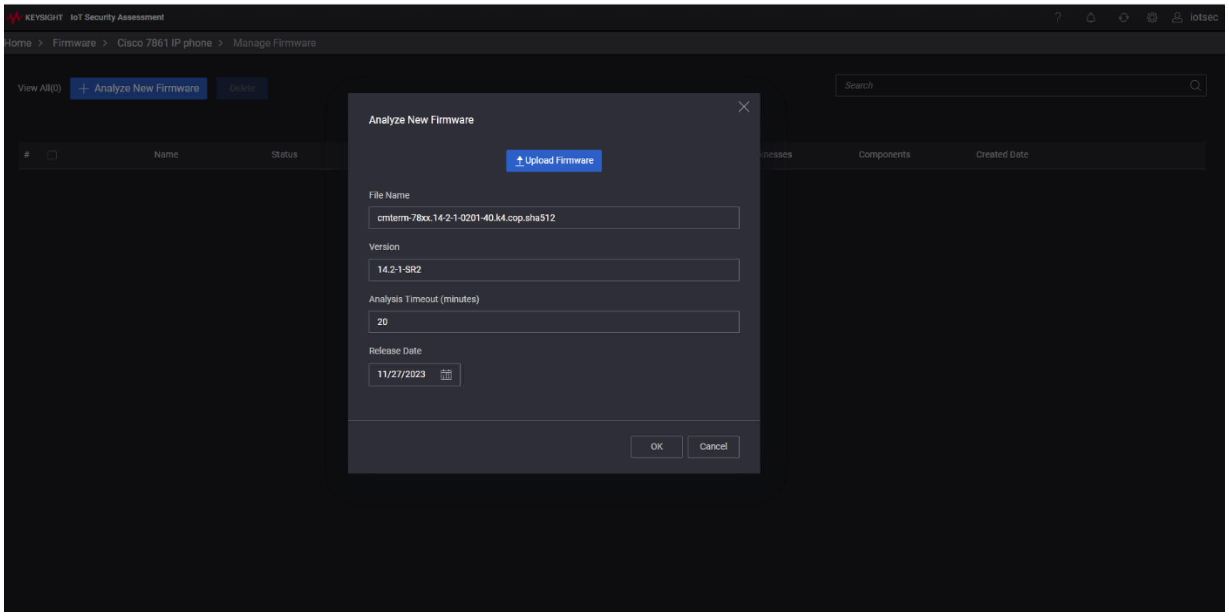
Manufacturer: Cisco

Model: 7861 IP phone

Select the product that you created to start firmware analysis and click "Firmware Analysis." On this page, you can manage already uploaded firmware, view the results of previously uploaded firmware, and analyze new firmware. To analyze new firmware, click on "Analyze New Firmware." Then click "Upload Firmware" and choose a binary firmware file from your system to upload. Enter the firmware version, analysis timeout, and input a release date.

The analysis timeout is set to 20 minutes by default, normally sufficient for firmware less than 100 MB on the Aveo Box hardware. However, if the size of your firmware file exceeds this limit or if you are using a less powerful system, you can increase the timeout.

After clicking "OK," the firmware will start uploading. When the upload finishes, the firmware upload box will close automatically, and the analysis will start immediately afterward. You can monitor the analysis status in the "Status" column. When the status changes to "Finished," the "Show Results" button is enabled, and you can click on it to view the analysis results.


KEYSIGHT IoT Security Assessment
iotsec
Home > Firmware > Cisco 7861 IP phone > Manage Firmware
View All(0)
+ Analyze New Firmware
Delete
Search
Upload Firmware
OK
Cancel

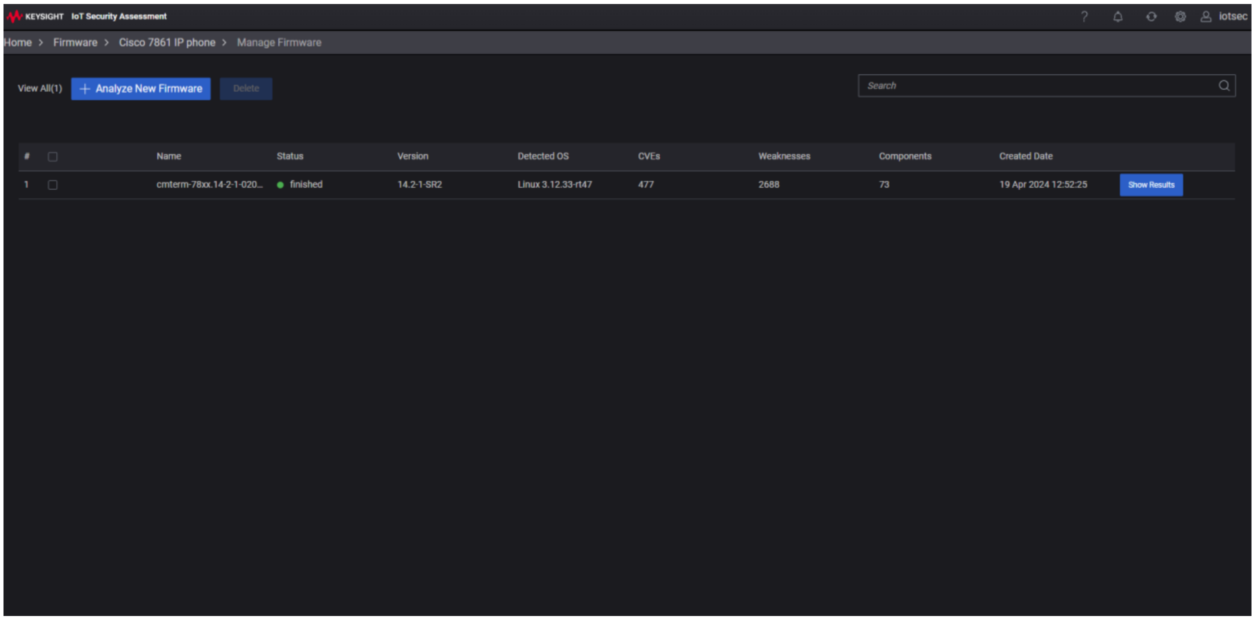
Analyze New Firmware

File Name: cmterm-78xx.14-2-1-0201-40.k4.cop.sha512

Version: 14.2-1-SR2

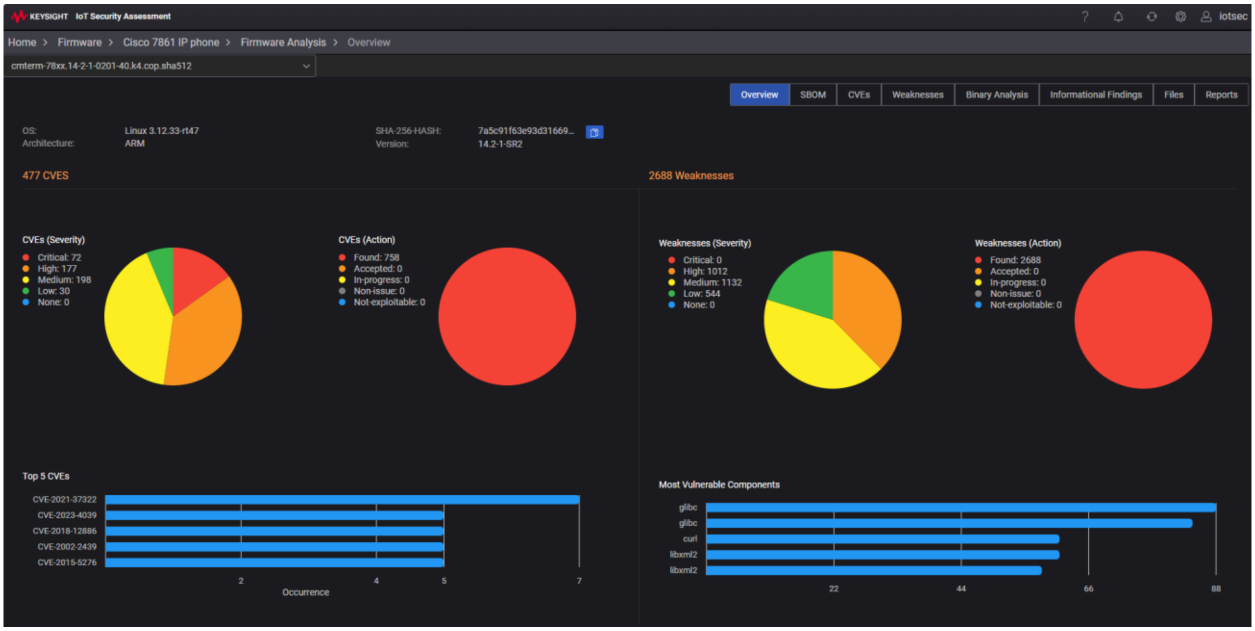
Analysis Timeout (minutes): 20

Release Date: 11/27/2023


KEYSIGHT IoT Security Assessment
iotsec
Home > Firmware > Cisco 7861 IP phone > Manage Firmware
View All(1)
+ Analyze New Firmware
Delete
Search

#	□	Name	Status	Version	Detected OS	CVEs	Weaknesses	Components	Created Date	
1	□	cmterm-78xx.14-2-1-020...	● finished	14.2-1-SR2	Linux 3.12.33-rt47	477	2688	73	19 Apr 2024 12:52:25	Show Results

As its name implies, the overview page provides an overview of the firmware that was analyzed. It displays general information about the firmware, such as the operating system, architecture, and SHA-2 hash. More importantly, it summarizes the analysis results in charts. For example, the CVEs (Severity) pie chart shows the number and proportion of CVEs identified in third-party components within the firmware, categorized by severity.



cmterm-78xx.14-2-1-0201-40.k4.cop.sha512

OS: Linux 3.12.33-rt47
Architecture: ARM
SHA-256-HASH: 7a5c91f63e93d31669...
Version: 14.2-1-SR2

477 CVES

CVEs (Severity)
Critical: 72
High: 177
Medium: 198
Low: 30
None: 0

CVEs (Action)
Found: 758
Accepted: 0
In-progress: 0
Non-issue: 0
Not-exploitable: 0

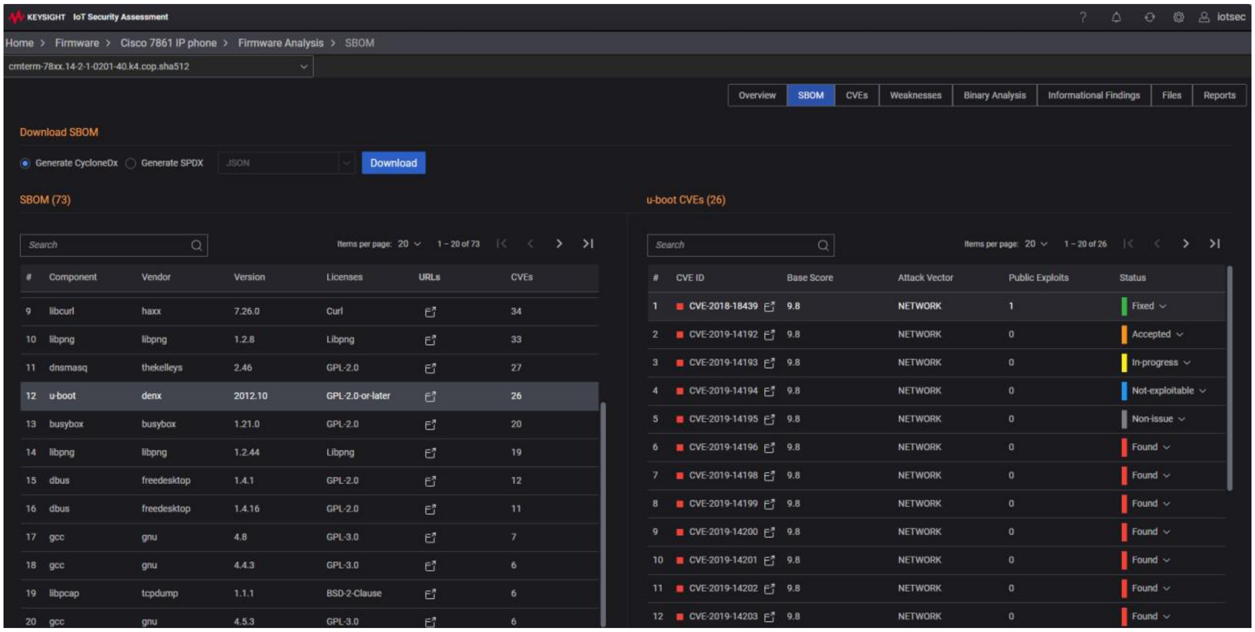
2688 Weaknesses

Weaknesses (Severity)
Critical: 0
High: 1012
Medium: 1132
Low: 544
None: 0

Weaknesses (Action)
Found: 2688
Accepted: 0
In-progress: 0
Non-issue: 0
Not-exploitable: 0

The SBOM page displays a list of components identified within the firmware and their associated CVEs. Most of these components are third-party components used by developers. It is important for manufacturers to maintain an updated list of these components and their associated CVEs and to stay informed whenever a new vulnerability is discovered in any of these components. One of the advantages of the Keysight product is the development of our own CVE search algorithm. This algorithm is designed to perform a nuanced correlation between components within the firmware and their associated CVEs, catching CVEs that other similar tools might miss and reducing false positives.

On this page, users can also generate and download SBOMs in SPDX and CycloneDX formats. SPDX and CycloneDX are standards for creating SBOMs that help manage software components. SPDX focuses more on licensing compliance, while CycloneDX emphasizes security, particularly in identifying vulnerabilities. These standards allow companies to easily share detailed information about their software components with customers or regulatory bodies. You can also integrate the files into various tools that automatically check for vulnerabilities or compliance issues.



SBOM (73)

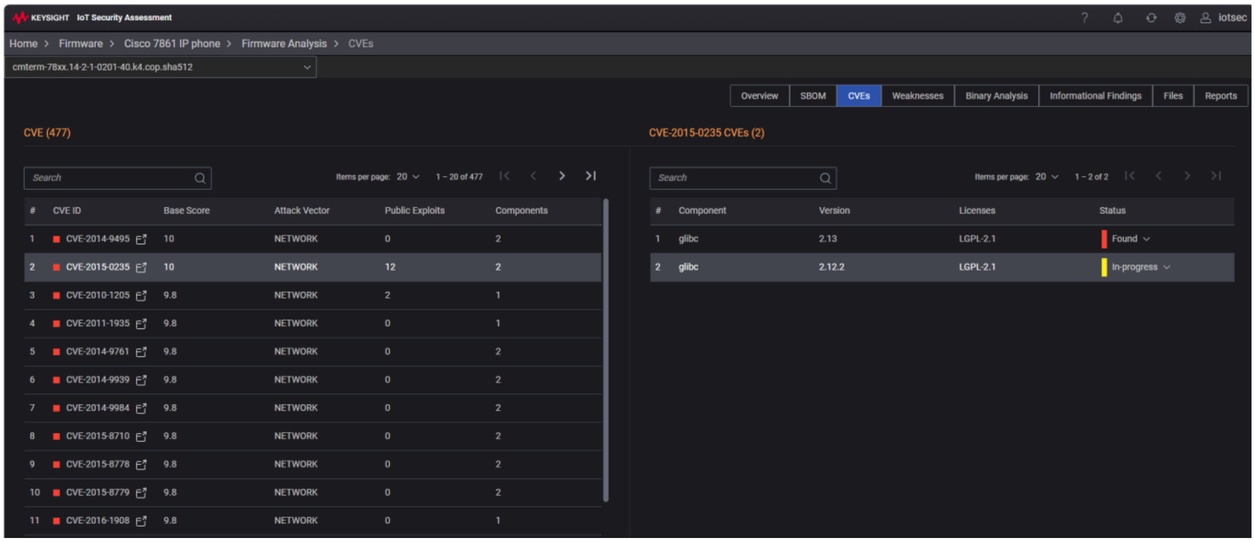
#	Component	Vendor	Version	Licenses	URLs	CVEs
9	libcurl	haxx	7.26.0	Curl		34
10	libpng	libpng	1.2.8	Libpng		33
11	dnsmasq	thekelleys	2.46	GPL-2.0		27
12	u-boot	denx	2012.10	GPL-2.0-or-later		26
13	busybox	busybox	1.21.0	GPL-2.0		20
14	libpng	libpng	1.2.44	Libpng		19
15	dbus	freedesktop	1.4.1	GPL-2.0		12
16	dbus	freedesktop	1.4.16	GPL-2.0		11
17	gcc	gnu	4.8	GPL-3.0		7
18	gcc	gnu	4.4.3	GPL-3.0		6
19	libpcap	tcpdump	1.1.1	BSD-2-Clause		6
20	gcc	gnu	4.5.3	GPL-3.0		6

u-boot CVEs (26)

#	CVE ID	Base Score	Attack Vector	Public Exploits	Status
1	CVE-2018-18439	9.8	NETWORK	1	Fixed
2	CVE-2019-14192	9.8	NETWORK	0	Accepted
3	CVE-2019-14193	9.8	NETWORK	0	In-progress
4	CVE-2019-14194	9.8	NETWORK	0	Not-exploitable
5	CVE-2019-14195	9.8	NETWORK	0	Non-issue
6	CVE-2019-14196	9.8	NETWORK	0	Found
7	CVE-2019-14198	9.8	NETWORK	0	Found
8	CVE-2019-14199	9.8	NETWORK	0	Found
9	CVE-2019-14200	9.8	NETWORK	0	Found
10	CVE-2019-14201	9.8	NETWORK	0	Found
11	CVE-2019-14202	9.8	NETWORK	0	Found
12	CVE-2019-14203	9.8	NETWORK	0	Found

The CVEs page lists all known vulnerabilities identified in firmware components. Since a product can have many components and, consequently, numerous CVEs, it might only be feasible to examine some of them. Also, some CVEs may not pose an issue on the target device or might not be exploitable. Therefore, you must be able to prioritize CVEs for remediation. The columns containing information such as the CVSS base score, the number of available public exploits, and the attack vector are vital for prioritizing these vulnerabilities effectively.

Moreover, the product allows you to change the status of a CVE from the default status of 'Found' to 'Fixed', 'Non-issue', 'Not exploitable', 'In-progress', or 'Accepted'. This feature allows you to track the status of a CVE in a component more efficiently.



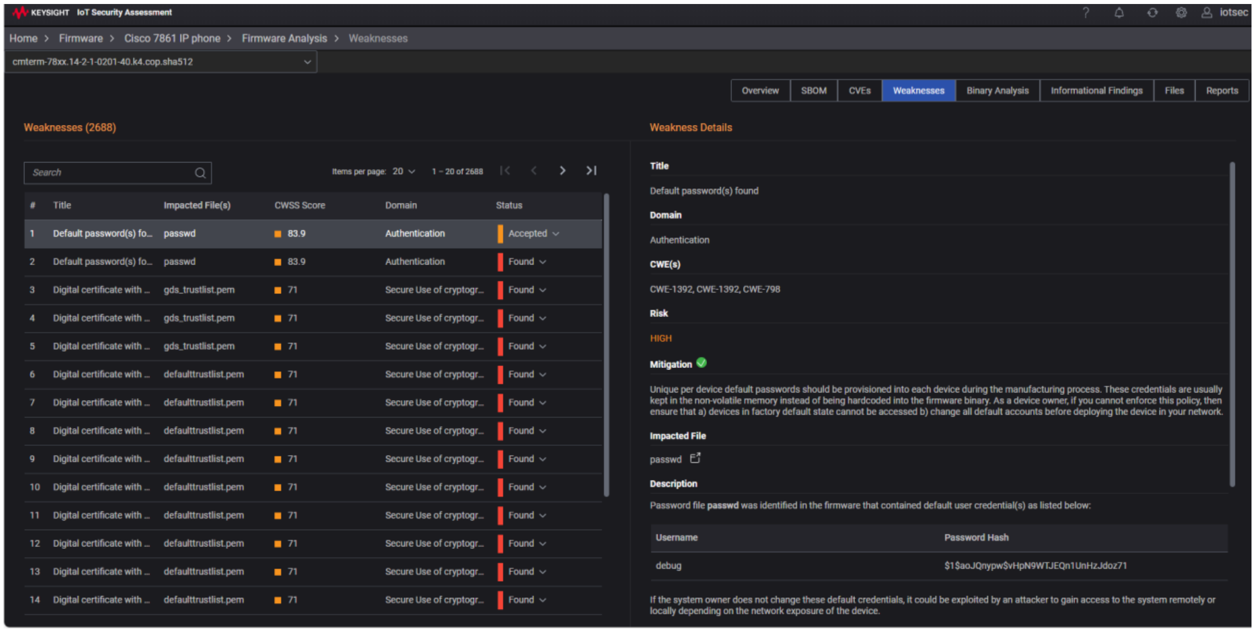
CVE (477)

#	CVE ID	Base Score	Attack Vector	Public Exploits	Components
1	CVE-2014-9495	10	NETWORK	0	2
2	CVE-2015-0235	10	NETWORK	12	2
3	CVE-2010-1205	9.8	NETWORK	2	1
4	CVE-2011-1935	9.8	NETWORK	0	1
5	CVE-2014-9761	9.8	NETWORK	0	2
6	CVE-2014-9939	9.8	NETWORK	0	2
7	CVE-2014-9984	9.8	NETWORK	0	2
8	CVE-2015-8710	9.8	NETWORK	0	2
9	CVE-2015-8778	9.8	NETWORK	0	2
10	CVE-2015-8779	9.8	NETWORK	0	2
11	CVE-2016-1908	9.8	NETWORK	0	1

CVE-2015-0235 CVEs (2)

#	Component	Version	Licenses	Status
1	glibc	2.13	LGPL-2.1	Found
2	glibc	2.12.2	LGPL-2.1	In-progress

In addition to known vulnerabilities or CVEs, firmware can exhibit various security issues, which we categorize under "Weaknesses." All of these are displayed on the Weaknesses page. These issues can range from default credentials, weak keys, and certificates to configuration issues in firmware operating systems or services. These weaknesses can be prioritized based on their Common Weakness Scoring System (CWSS). For every weakness, the system provides the domain, impacted file, risk level, detailed description, attack condition, exploitation impact, and, most importantly, mitigation strategies. Similar to CVEs, each weakness has a status that users can change to easily track their resolution progress.


KEYSIGHT IoT Security Assessment
iotsec
Home > Firmware > Cisco 7861 IP phone > Firmware Analysis > Weaknesses
cmterm-78xx.14-2-1-0201-40.k4.cop.sha512
Overview
SBOM
CVEs
Weaknesses
Binary Analysis
Informational Findings
Files
Reports
Search
Items per page: 20
1 – 20 of 2688

Weaknesses (2688)

#	Title	Impacted File(s)	CWSS Score	Domain	Status
1	Default password(s) fo...	passwd	83.9	Authentication	Accepted
2	Default password(s) fo...	passwd	83.9	Authentication	Found
3	Digital certificate with ...	gds_trustlist.pem	71	Secure Use of cryptogr...	Found
4	Digital certificate with ...	gds_trustlist.pem	71	Secure Use of cryptogr...	Found
5	Digital certificate with ...	gds_trustlist.pem	71	Secure Use of cryptogr...	Found
6	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
7	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
8	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
9	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
10	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
11	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
12	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
13	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found
14	Digital certificate with ...	defaulttrustlist.pem	71	Secure Use of cryptogr...	Found

Weakness Details

Title

Default password(s) found

Domain

Authentication

CWE(s)

CWE-1392, CWE-1392, CWE-798

Risk

HIGH

Mitigation ✓

Unique per device default passwords should be provisioned into each device during the manufacturing process. These credentials are usually kept in the non-volatile memory instead of being hardcoded into the firmware binary. As a device owner, if you cannot enforce this policy, then ensure that a) devices in factory default state cannot be accessed b) change all default accounts before deploying the device in your network.

Impacted File

passwd

Description

Password file **passwd** was identified in the firmware that contained default user credential(s) as listed below:

Username	Password Hash
debug	$1$aoJQnypw$vHpN9WTJEQn1UnHzJdoz71

If the system owner does not change these default credentials, it could be exploited by an attacker to gain access to the system remotely or locally depending on the network exposure of the device.

FAQs

1. **Can the Keysight solution integrate with existing development and security workflows?** Yes, the Keysight solution comes with API support that allows it to seamlessly integrate into automated workflows and systems, facilitating continuous and automated security analysis within the development pipeline.

2. **What measures are in place to ensure the confidentiality of analyzed firmware?** Keysight is committed to maintaining the confidentiality of firmware data. The Keysight solution is delivered as a physical appliance, which is deployed on the customer's premises, ensuring that all firmware data remains within their secure environment. This setup guarantees that no firmware data is transmitted outside, thus maintaining its confidentiality. Additionally, the Keysight solution is designed not to collect any customer data, offering an extra layer of security and privacy protection for our clients' sensitive information.

3. **What types of IoT firmware can the solution analyze?** The Keysight solution supports various firmware architectures and operating systems, such as Linux/Android and bare-metal based on ARM-Cortex-M architecture.

4. **Are there any limitations on the size or complexity of the firmware that I can analyze?** The Keysight solution currently accommodates binary firmware of a maximum of 2 GB and supports over 30 widely used firmware file system formats, catering to a wide range of devices and applications. However, the solution does not currently support the extraction of proprietary file system firmware formats or firmware files that are encrypted or obfuscated. This limitation is due to the specific challenges associated with accessing and analyzing the content of these formats without the necessary decryption keys or format specifications.

5. **What sets your solution apart from competitors?** The Keysight solution uniquely supports firmware analysis for ARM-Cortex-M based firmware, which is prevalent in approximately 90% of battery-powered devices. Additionally, Keysight offers a comprehensive package that combines firmware analysis with IoT active vulnerability analysis over the network, and generational fuzzing. This all-inclusive approach is not matched by any competitor, providing Keysight clients with unparalleled insights and security coverage for their devices.

6. **How long does it typically take to analyze a firmware with the solution?** Analysis time can vary depending on the complexity and size of the firmware. However, the Keysight solution is optimized for efficiency, and most analyses are completed within a few minutes, providing quick insights into potential vulnerabilities.

Conclusion

This application note discusses the unique role of firmware in IoT devices and how it presents distinct security challenges. Traditional security measures often overlook firmware, leaving vulnerabilities unaddressed. The Keysight solution fills this gap, offering deep firmware analysis capabilities from SBOM generation to vulnerability detection and beyond, ensuring comprehensive device security.

For developers, security analysts, and decision-makers who must elevate the security of their IoT devices, Keysight's Automated IoT Firmware Security Analysis Solution—part of the Keysight IoT Security Assessment product — presents a strategic advantage. Consider how integrating this solution into your security workflow can protect your devices, safeguard your brand's reputation, and open up new market opportunities. Contact the Keysight team for more information and take a proactive step toward securing your IoT device.

This information is subject to change without notice. © Keysight Technologies, 2024,
Published in USA, May 6, 2024, 3124-1348.EN