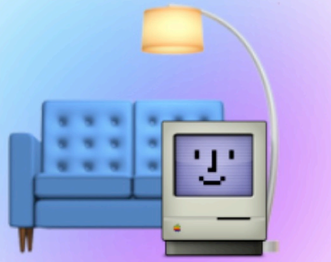
Exploring SOFA

Simple Organized Feed for Apple Software Updates



MacAdmins Meeting - August 2024

Henry Stamerjohann - Zentral (Co-Founder)

https://apple.lib.utah.edu/August-2024-macadmins-meeting/

Agenda

Exploring SOFA

Introduction to SOFA

Pain Points

Key Benefits

Origin and Evolution

Integrations & Ecosystem

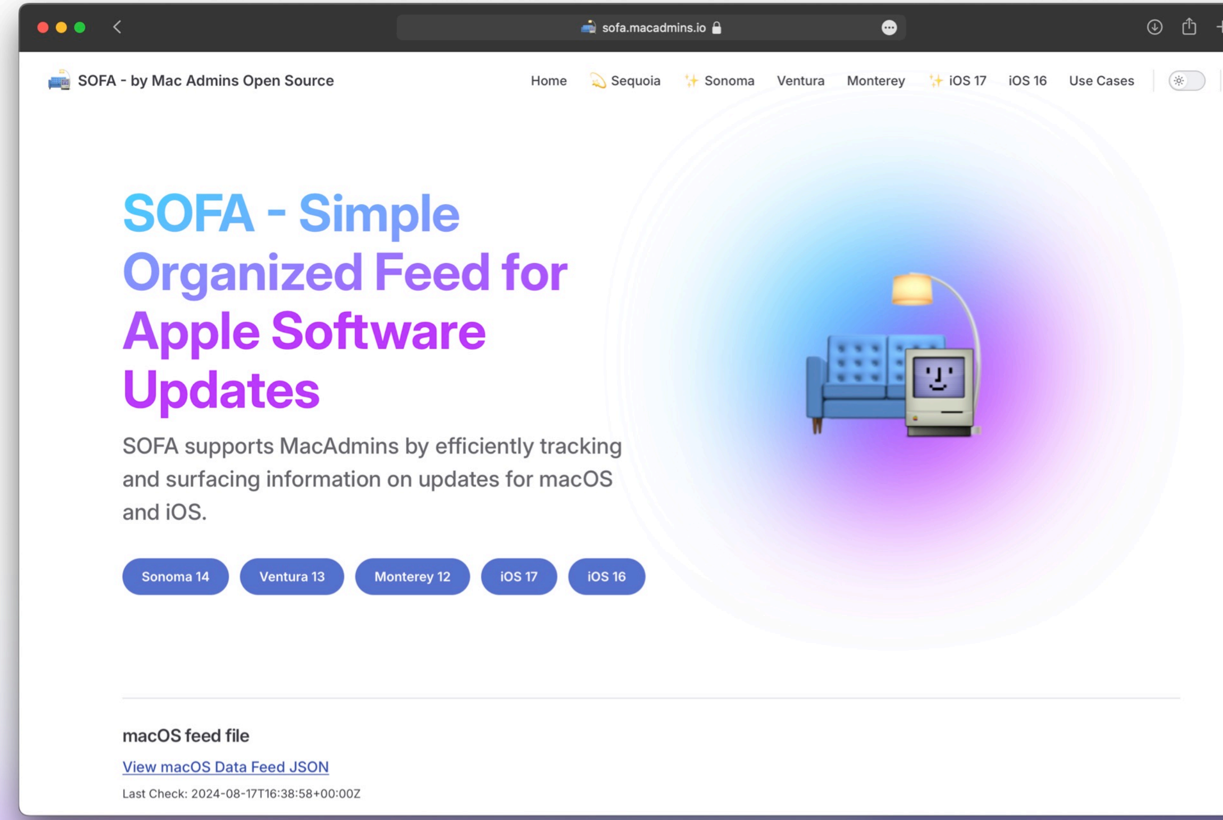
Self-Hosting & Future Directions

Introduction to SOFA

Overview

Web UI

Machine readable feed



SOFA - Simple Organized Feed for Apple Software Updates

SOFA supports MacAdmins by efficiently tracking and surfacing information on updates for macOS and iOS.

macOS feed file

View macOS Data Feed JSON

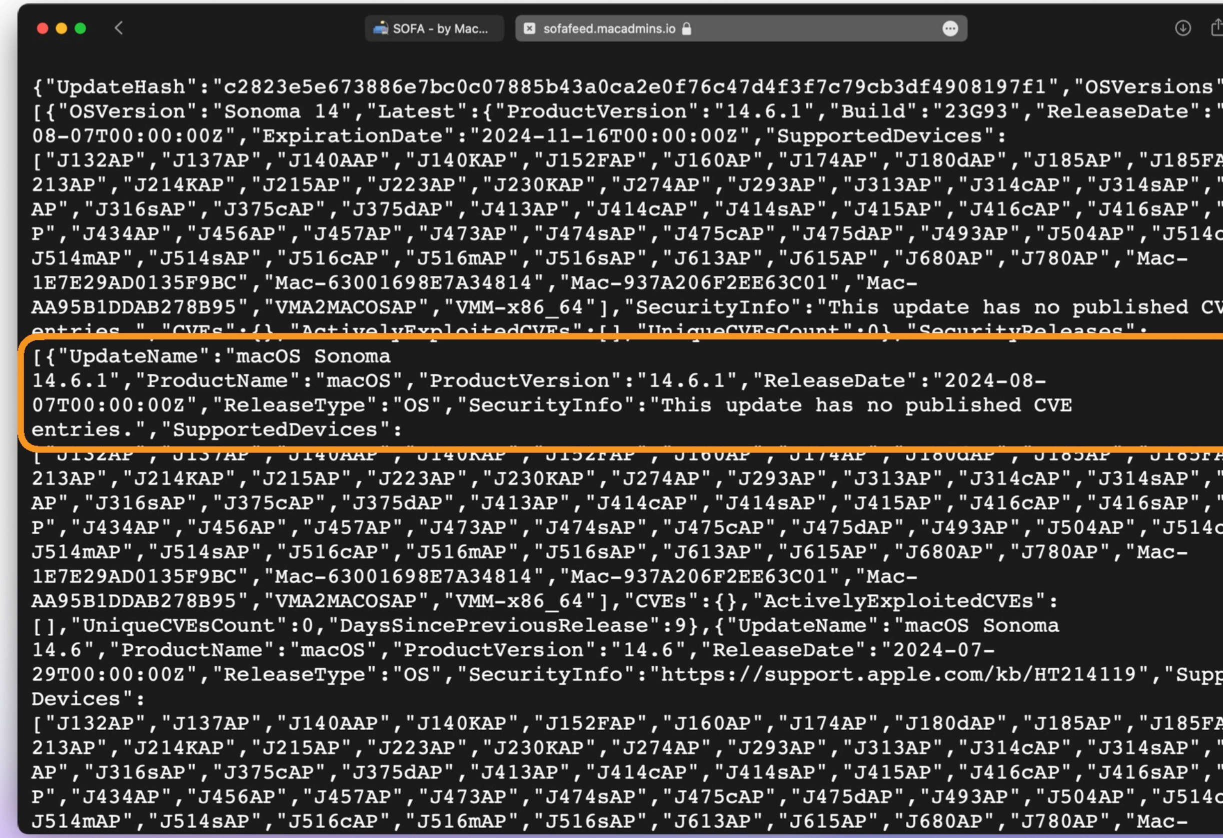
Last Check: 2024-08-17T16:38:58+00:00Z

Introduction to SOFA

Overview

Web UI

Machine readable feed



```
{"UpdateHash":"c2823e5e673886e7bc0c07885b43a0ca2e0f76c47d4f3f7c79cb3df4908197f1","OSVersions"
[{"OSVersion":"Sonoma 14","Latest":{"ProductVersion":"14.6.1","Build":"23G93","ReleaseDate":"
08-07T00:00:00Z","ExpirationDate":"2024-11-16T00:00:00Z","SupportedDevices":
["J132AP","J137AP","J140AAP","J140KAP","J152FAP","J160AP","J174AP","J180dAP","J185AP","J185FA
213AP","J214KAP","J215AP","J223AP","J230KAP","J274AP","J293AP","J313AP","J314cAP","J314sAP","
AP","J316sAP","J375cAP","J375dAP","J413AP","J414cAP","J414sAP","J415AP","J416cAP","J416sAP","
P","J434AP","J456AP","J457AP","J473AP","J474sAP","J475cAP","J475dAP","J493AP","J504AP","J514c
J514mAP","J514sAP","J516cAP","J516mAP","J516sAP","J613AP","J615AP","J680AP","J780AP","Mac-
1E7E29AD0135F9BC","Mac-63001698E7A34814","Mac-937A206F2EE63C01","Mac-
AA95B1DDAB278B95","VMA2MACOSAP","VMM-x86_64"],"SecurityInfo":"This update has no published CV
entries.","CVEs":{},"ActivelyExploitedCVEs":[],"UniqueCVEsCount":0},"SecurityReleases":
[{"UpdateName":"macOS Sonoma
14.6.1","ProductName":"macOS","ProductVersion":"14.6.1","ReleaseDate":"2024-08-
07T00:00:00Z","ReleaseType":"OS","SecurityInfo":"This update has no published CVE
entries.","SupportedDevices":
["J132AP","J137AP","J140AAP","J140KAP","J152FAP","J160AP","J174AP","J180dAP","J185AP","J185FA
213AP","J214KAP","J215AP","J223AP","J230KAP","J274AP","J293AP","J313AP","J314cAP","J314sAP","
AP","J316sAP","J375cAP","J375dAP","J413AP","J414cAP","J414sAP","J415AP","J416cAP","J416sAP","
P","J434AP","J456AP","J457AP","J473AP","J474sAP","J475cAP","J475dAP","J493AP","J504AP","J514c
J514mAP","J514sAP","J516cAP","J516mAP","J516sAP","J613AP","J615AP","J680AP","J780AP","Mac-
1E7E29AD0135F9BC","Mac-63001698E7A34814","Mac-937A206F2EE63C01","Mac-
AA95B1DDAB278B95","VMA2MACOSAP","VMM-x86_64"],"CVEs":{},"ActivelyExploitedCVEs":
[],"UniqueCVEsCount":0,"DaysSincePreviousRelease":9},{"UpdateName":"macOS Sonoma
14.6","ProductName":"macOS","ProductVersion":"14.6","ReleaseDate":"2024-07-
29T00:00:00Z","ReleaseType":"OS","SecurityInfo":"https://support.apple.com/kb/HT214119","Supp
Devices":
["J132AP","J137AP","J140AAP","J140KAP","J152FAP","J160AP","J174AP","J180dAP","J185AP","J185FA
213AP","J214KAP","J215AP","J223AP","J230KAP","J274AP","J293AP","J313AP","J314cAP","J314sAP","
AP","J316sAP","J375cAP","J375dAP","J413AP","J414cAP","J414sAP","J415AP","J416cAP","J416sAP","
P","J434AP","J456AP","J457AP","J473AP","J474sAP","J475cAP","J475dAP","J493AP","J504AP","J514c
J514mAP","J514sAP","J516cAP","J516mAP","J516sAP","J613AP","J615AP","J680AP","J780AP","Mac-
```

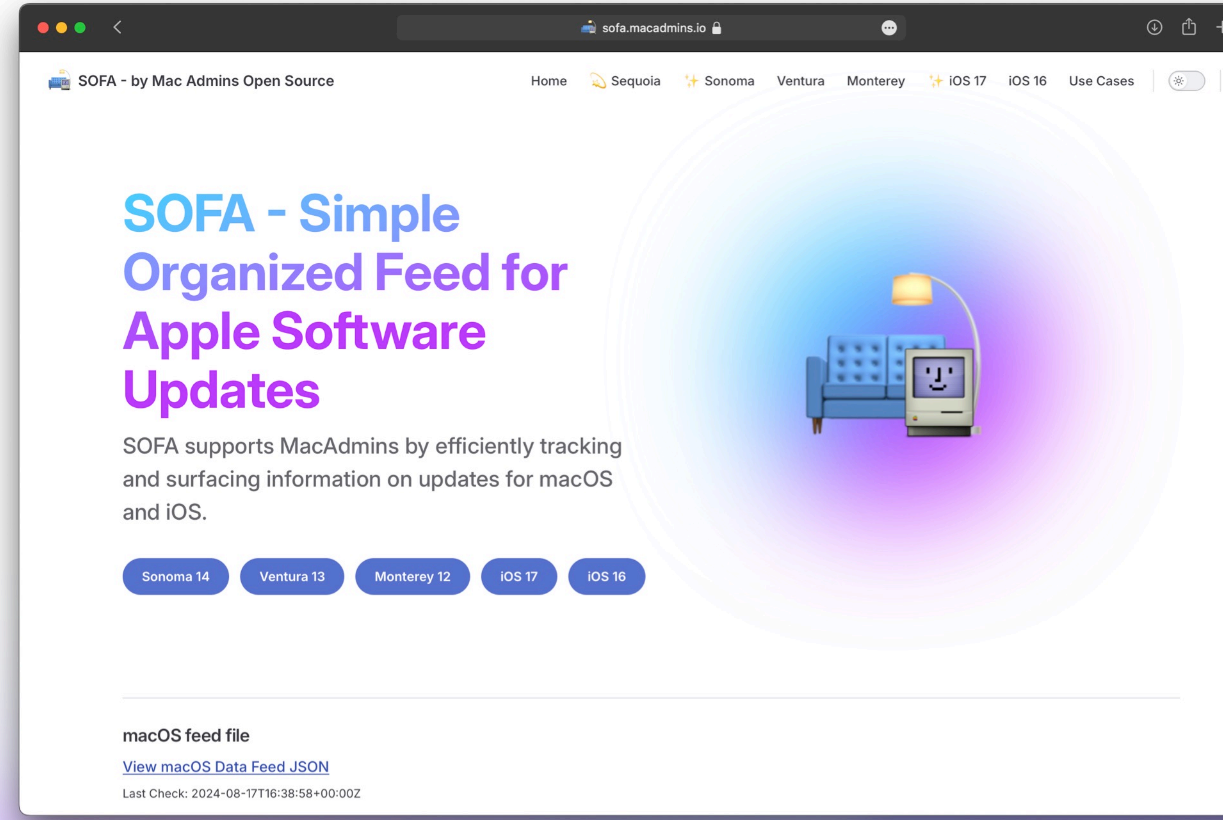
Introduction to SOFA

Overview

Web UI

Machine readable feed

Essential use case:
Informal & compliance workflows



SOFA - Simple Organized Feed for Apple Software Updates

SOFA supports MacAdmins by efficiently tracking and surfacing information on updates for macOS and iOS.

macOS feed file

View macOS Data Feed JSON

Last Check: 2024-08-17T16:38:58+00:00Z

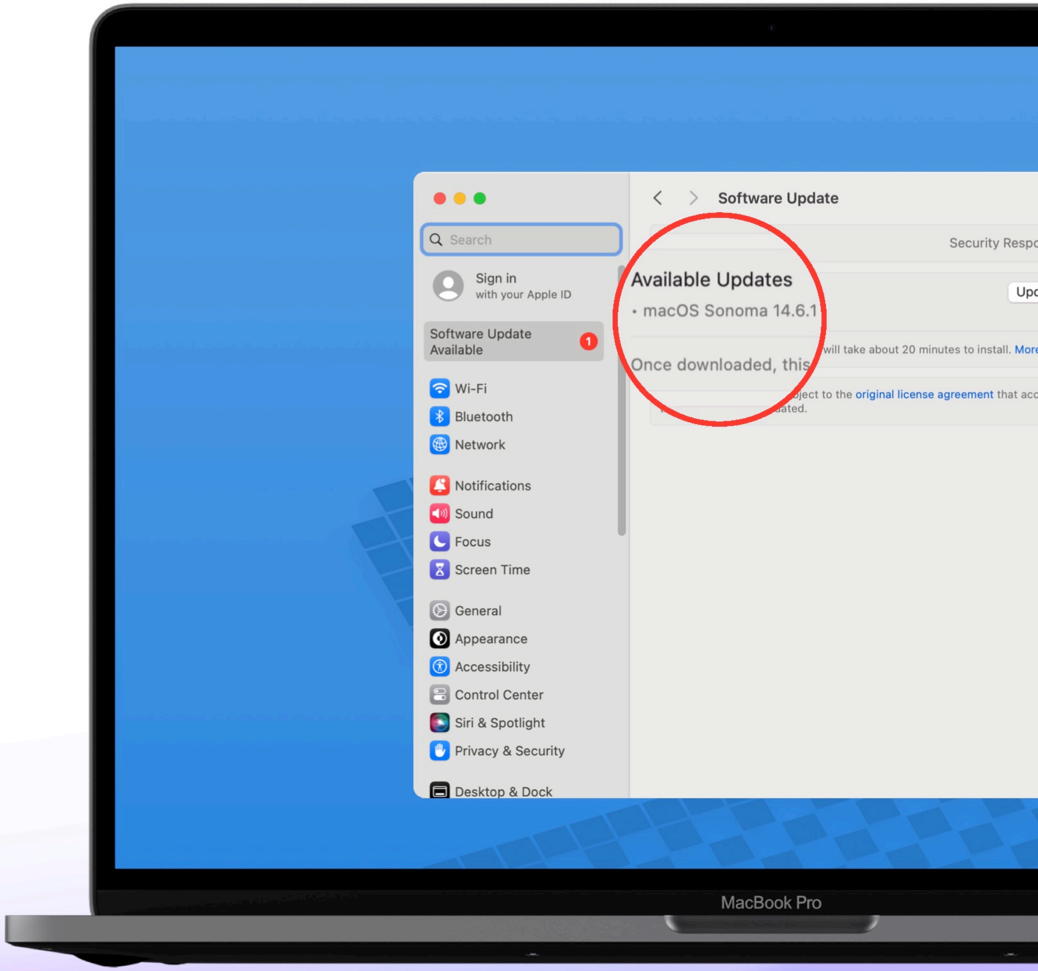
Pain Points

SLA pressure

Endpoint protection, stay compliant

Patch critical OS security vulnerabilities

Get OS data and release history efficiently



Available Updates

- macOS Sonoma 14.6.1

Once downloaded, this will take about 20 minutes to install. More

bject to the original license agreement that acc

dated.

Key Benefits

The objective of SOFA

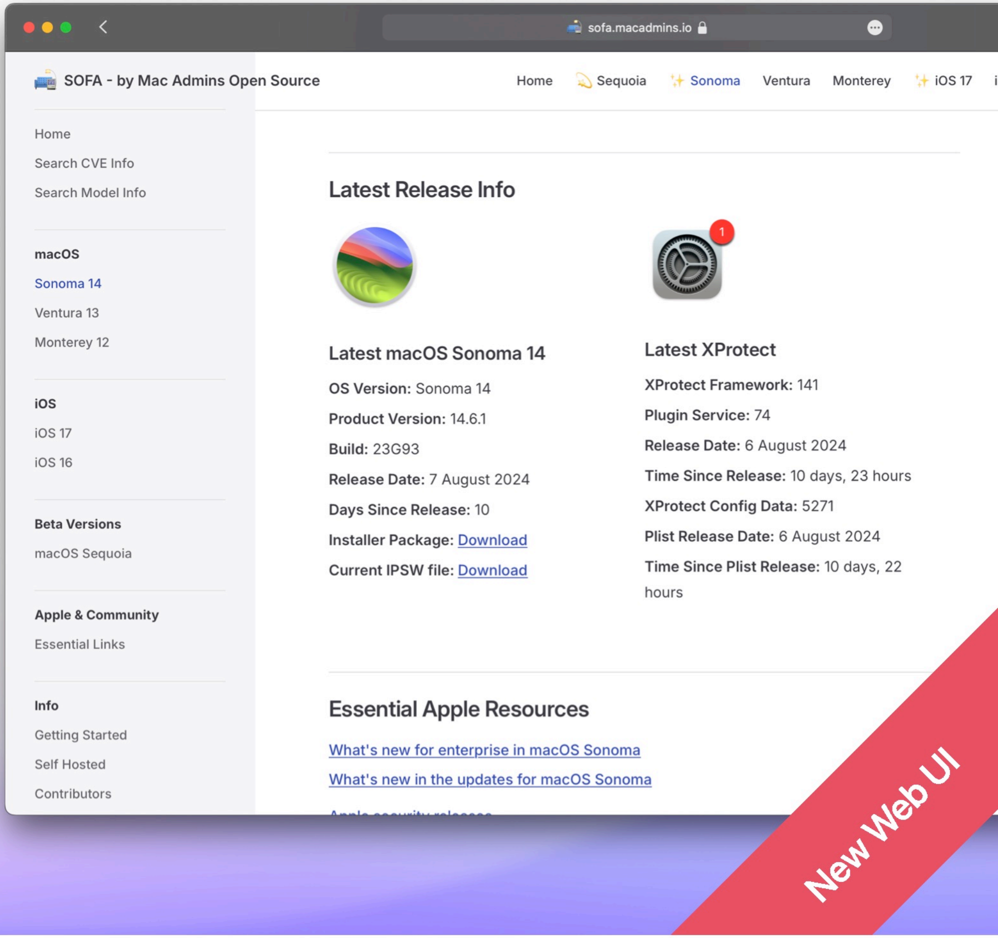
Canonical source of truth

Release awareness

Patch & SLA reference

Easier access than GDMF

Community-driven tool



Latest Release Info

Latest macOS Sonoma 14

OS Version: Sonoma 14
Product Version: 14.6.1
Build: 23G93
Release Date: 7 August 2024
Days Since Release: 10
Installer Package: Download
Current IPSW file: Download

Latest XProtect

XProtect Framework: 141
Plugin Service: 74
Release Date: 6 August 2024
Time Since Release: 10 days, 23 hours
XProtect Config Data: 5271
Plist Release Date: 6 August 2024
Time Since Plist Release: 10 days, 22 hours

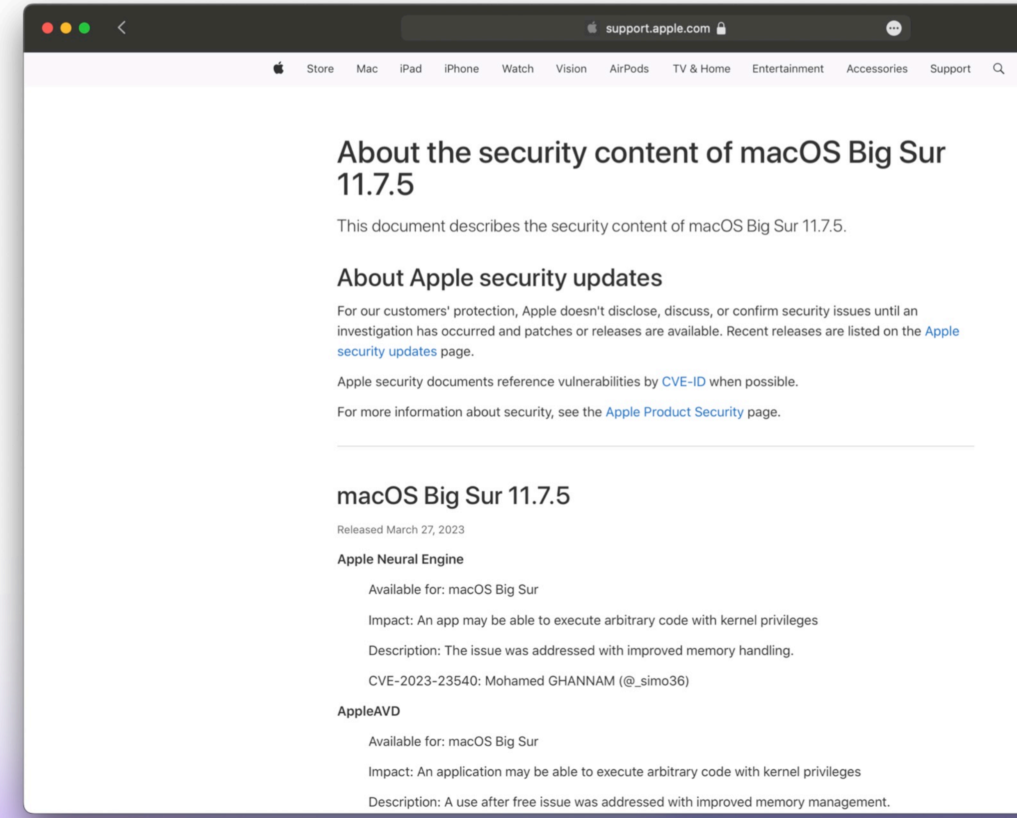
Essential Apple Resources

What's new for enterprise in macOS Sonoma
What's new in the updates for macOS Sonoma
Apple security releases

Origin and Evolution

How SOFA started...

Back in the days... manual data evaluation



About the security content of macOS Big Sur 11.7.5

This document describes the security content of macOS Big Sur 11.7.5.

About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security updates page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

macOS Big Sur 11.7.5

Released March 27, 2023

Apple Neural Engine

Available for: macOS Big Sur

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: The issue was addressed with improved memory handling.

CVE-2023-23540: Mohamed GHANNAM (@_simo36)

AppleAVD

Available for: macOS Big Sur

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A use after free issue was addressed with improved memory management.

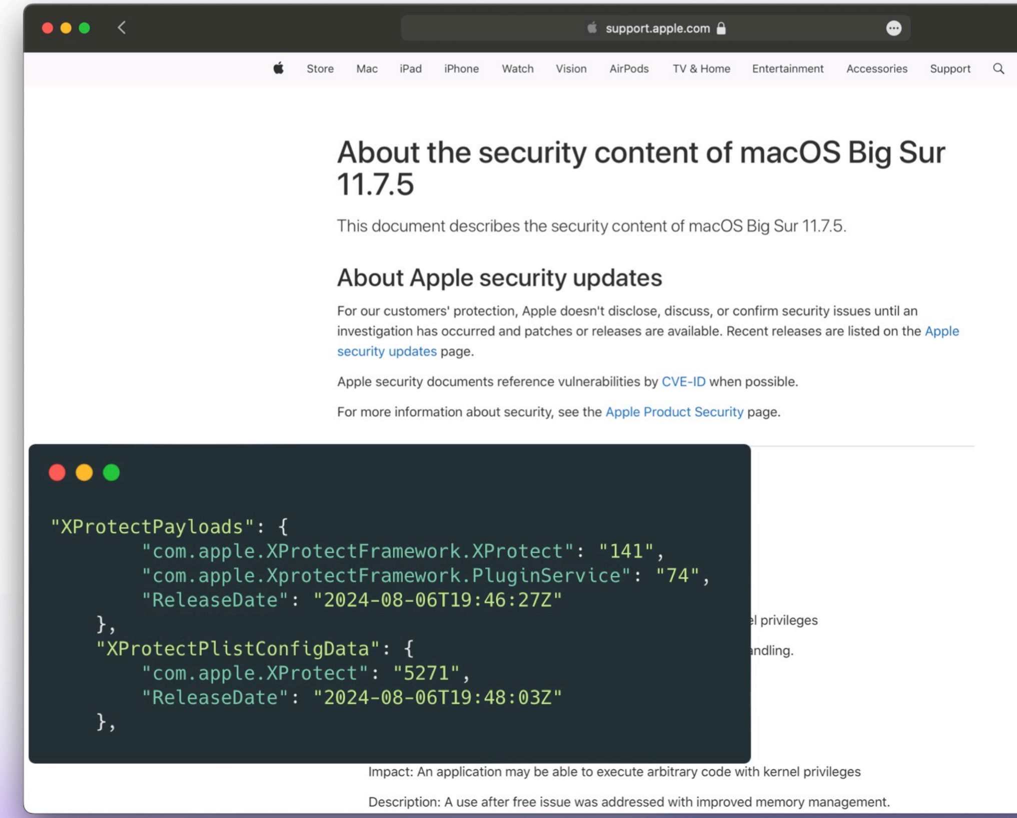
Origin and Evolution

How SOFA started...

Back in the days... manual data evaluation

Xprotect reference was needed

[e.g. CIS 5.10 Ensure XProtect Is Running and Updated (Automated)]



About the security content of macOS Big Sur 11.7.5

This document describes the security content of macOS Big Sur 11.7.5.

About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security updates page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

l privileges

ndling.

```
"XProtectPayloads": {
        "com.apple.XProtectFramework.XProtect": "141",
        "com.apple.XprotectFramework.PluginService": "74",
        "ReleaseDate": "2024-08-06T19:46:27Z"
    },
    "XProtectPlistConfigData": {
        "com.apple.XProtect": "5271",
        "ReleaseDate": "2024-08-06T19:48:03Z"
    },
```

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A use after free issue was addressed with improved memory management.

Origin and Evolution

How SOFA started...

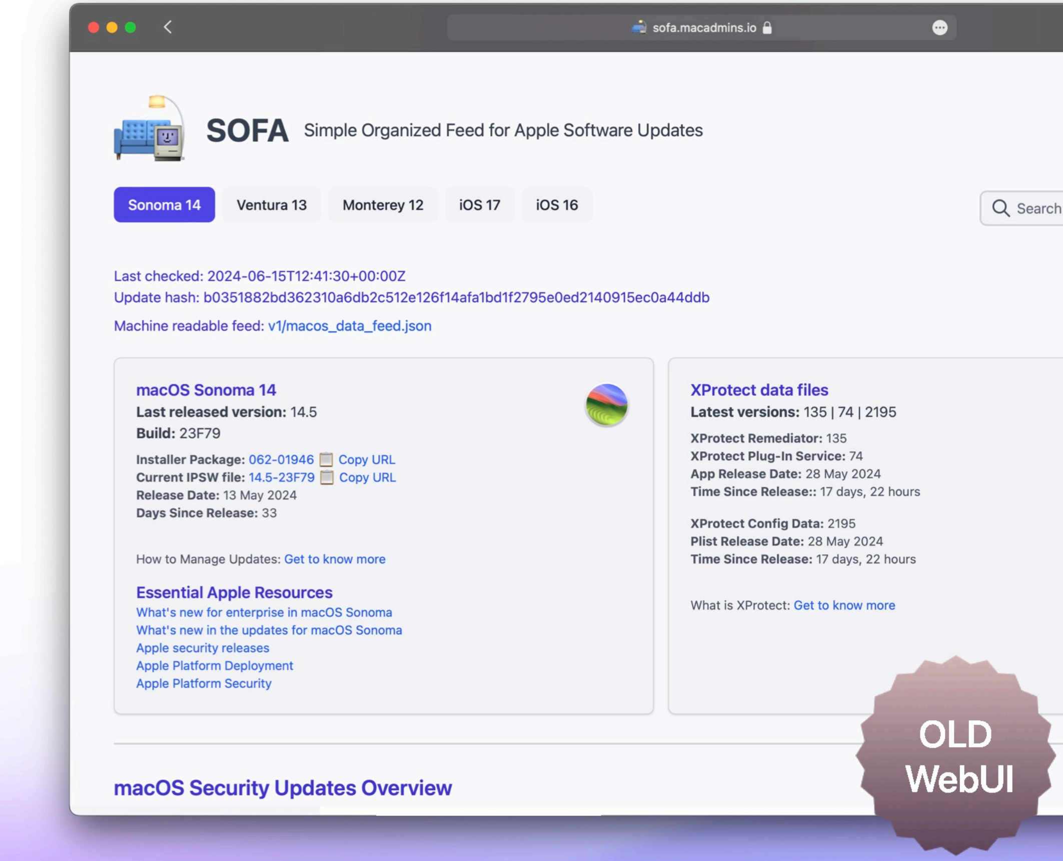
Back in the days... manual data evaluation

Xprotect reference was needed

[e.g. CIS 5.10 Ensure XProtect Is Running and Updated (Automated)]

Automated JSON aggregation

Feedback shaped SOFA



SOFA Simple Organized Feed for Apple Software Updates

Last checked: 2024-06-15T12:41:30+00:00Z
Update hash: b0351882bd362310a6db2c512e126f14afa1bd1f2795e0ed2140915ec0a44ddb

Machine readable feed: v1/macos_data_feed.json

macOS Sonoma 14
Last released version: 14.5
Build: 23F79
Installer Package: 062-01946 📋 Copy URL
Current IPSW file: 14.5-23F79 📋 Copy URL
Release Date: 13 May 2024
Days Since Release: 33

How to Manage Updates: Get to know more

Essential Apple Resources
What's new for enterprise in macOS Sonoma
What's new in the updates for macOS Sonoma
Apple security releases
Apple Platform Deployment
Apple Platform Security

XProtect data files
Latest versions: 135 | 74 | 2195
XProtect Remediator: 135
XProtect Plug-In Service: 74
App Release Date: 28 May 2024
Time Since Release:: 17 days, 22 hours

XProtect Config Data: 2195
Plist Release Date: 28 May 2024
Time Since Release: 17 days, 22 hours

What is XProtect: Get to know more

macOS Security Updates Overview

OLD WebUI

Origin and Evolution

How SOFA started...

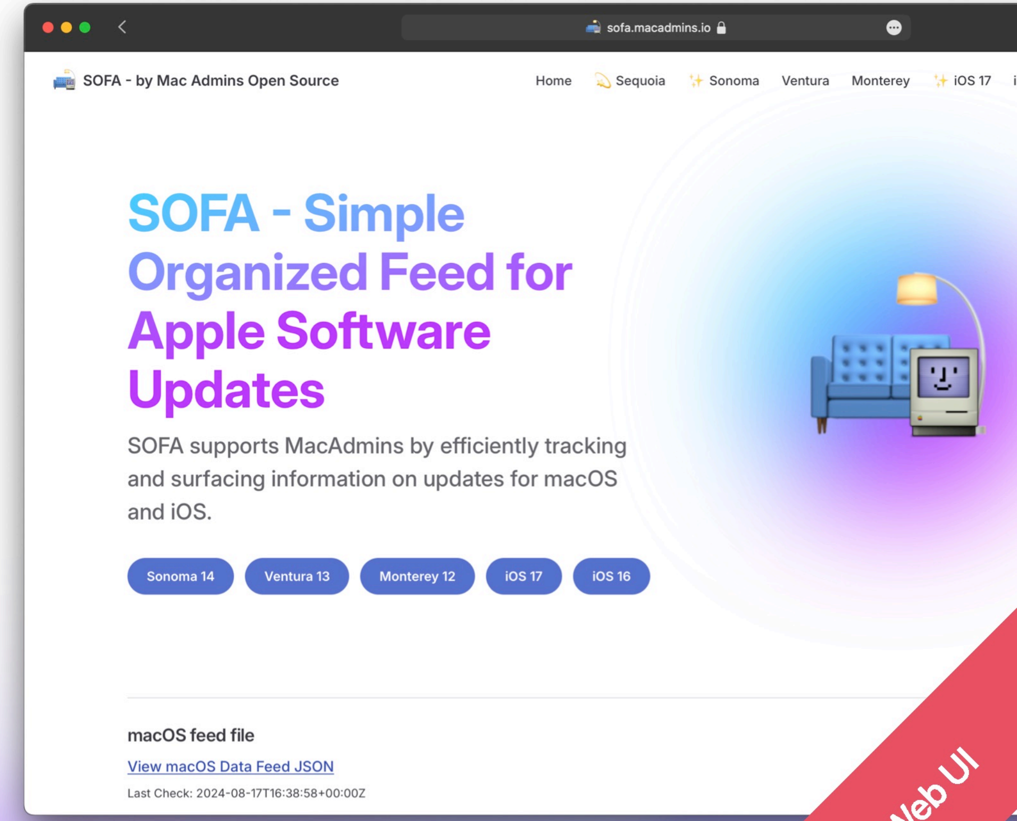
Back in the days... manual data evaluation

Xprotect reference was needed
[e.g. CIS 5.10 Ensure XProtect Is Running and Updated (Automated)]

Automated JSON aggregation

Feedback shaped SOFA

New UI and ecosystem growth



SOFA - Simple Organized Feed for Apple Software Updates

SOFA supports MacAdmins by efficiently tracking and surfacing information on updates for macOS and iOS.

macOS feed file

View macOS Data Feed JSON

Last Check: 2024-08-17T16:38:58+00:00Z

New Web UI

DEMO - Web UI and Tools

SOFA UI and features

Key integrations

Security and patch info

Integrations & Ecosystem

Key integrations

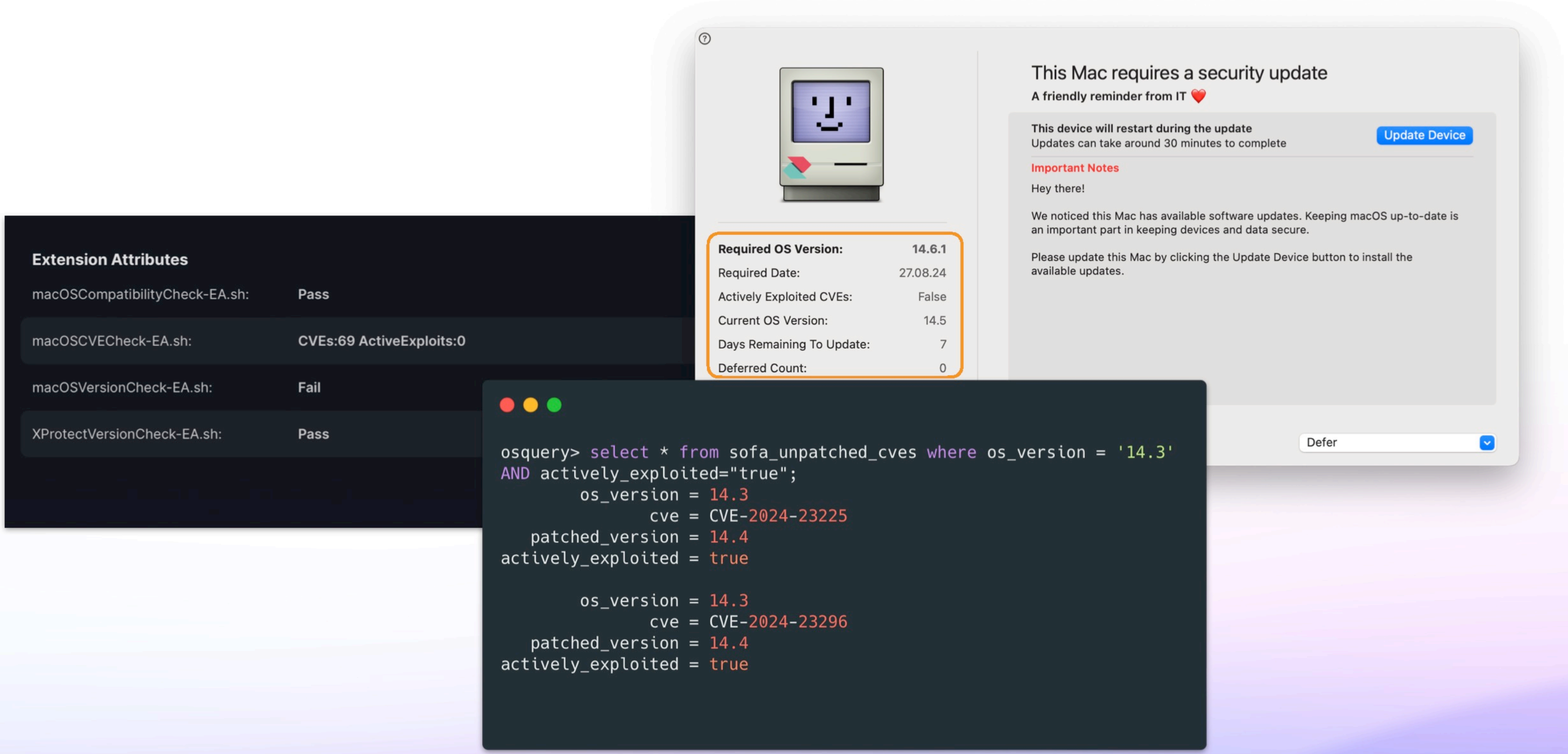
Osquery

Nudge 2.0

Jamf EAs

Tags

Scripts



Extension Attributes

macOSCompatibilityCheck-EA.sh:	Pass
macOSCVECheck-EA.sh:	CVEs:69 ActiveExploits:0
macOSVersionCheck-EA.sh:	Fail
XProtectVersionCheck-EA.sh:	Pass

This Mac requires a security update

A friendly reminder from IT ❤️

This device will restart during the update
Updates can take around 30 minutes to complete

Important Notes

Hey there!

We noticed this Mac has available software updates. Keeping macOS up-to-date is an important part in keeping devices and data secure.

Please update this Mac by clicking the Update Device button to install the available updates.

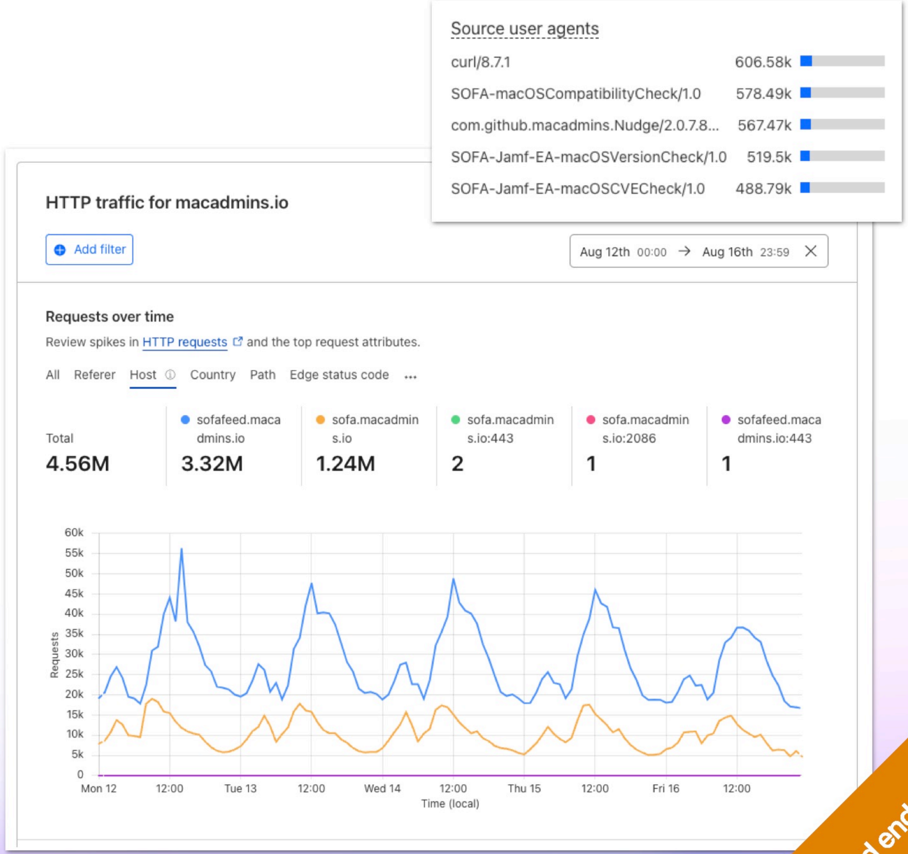
Required OS Version:	14.6.1
Required Date:	27.08.24
Actively Exploited CVEs:	False
Current OS Version:	14.5
Days Remaining To Update:	7
Deferred Count:	0

```
osquery> select * from sofa_unpatched_cves where os_version = '14.3'
AND actively_exploited="true";
        os_version = 14.3
               cve = CVE-2024-23225
   patched_version = 14.4
actively_exploited = true

        os_version = 14.3
               cve = CVE-2024-23296
   patched_version = 14.4
actively_exploited = true
```

Self-Hosting & Future Directions

Community vs. Self-hosted - why ?



Source user agents

curl/8.7.1	606.58k
SOFA-macOSCompatibilityCheck/1.0	578.49k
com.github.macadmins.Nudge/2.0.7.8...	567.47k
SOFA-Jamf-EA-macOSVersionCheck/1.0	519.5k
SOFA-Jamf-EA-macOSCVECheck/1.0	488.79k

HTTP traffic for macadmins.io

Add filter

Aug 12th 00:00 → Aug 16th 23:59

Requests over time

Review spikes in HTTP requests and the top request attributes.

All Referer Host Country Path Edge status code ...

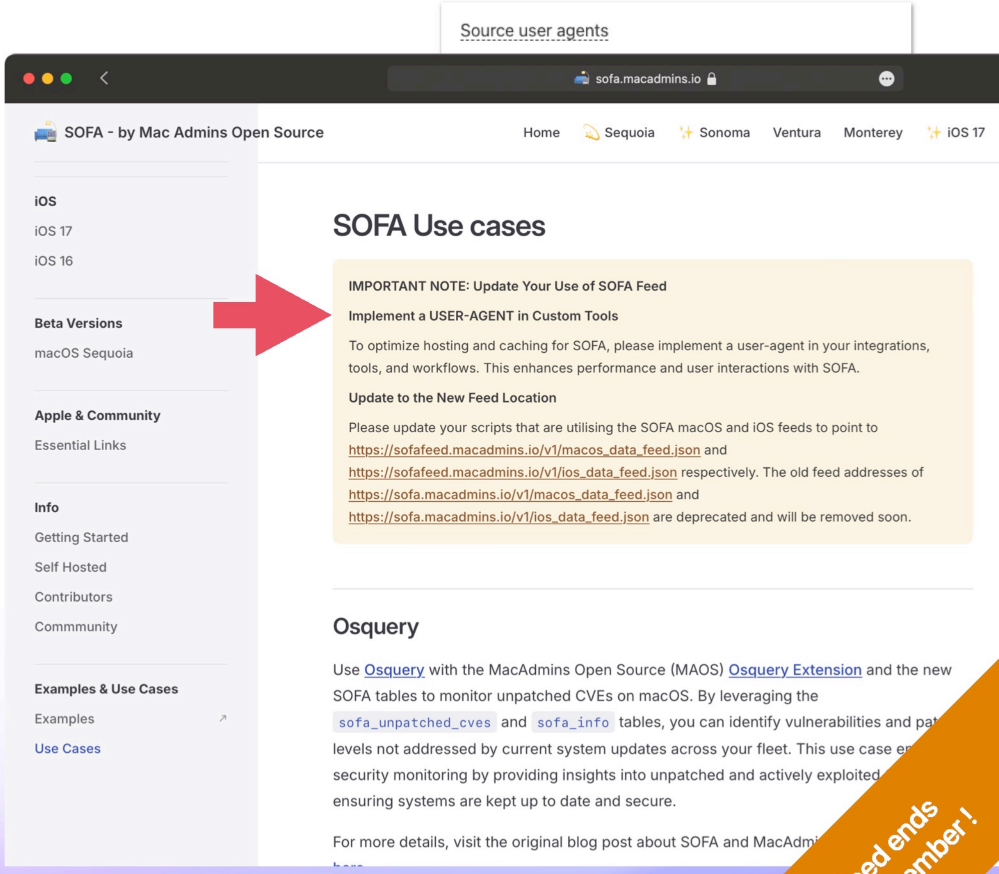
Total	● sofafeed.macadmins.io	● sofa.macadmins.io	● sofa.macadmins.io:443	● sofa.macadmins.io:2086	● sofafeed.macadmins.io:443
4.56M	3.32M	1.24M	2	1	1

Old feed ends on 2 September !

Self-Hosting & Future Directions

Community vs. Self-hosted - why ?

Implement a USER-AGENT in Custom Tools



SOFA Use cases

IMPORTANT NOTE: Update Your Use of SOFA Feed

Implement a USER-AGENT in Custom Tools

To optimize hosting and caching for SOFA, please implement a user-agent in your integrations, tools, and workflows. This enhances performance and user interactions with SOFA.

Update to the New Feed Location

Please update your scripts that are utilising the SOFA macOS and iOS feeds to point to https://sofafeed.macadmins.io/v1/macos_data_feed.json and https://sofafeed.macadmins.io/v1/ios_data_feed.json respectively. The old feed addresses of https://sofa.macadmins.io/v1/macos_data_feed.json and https://sofa.macadmins.io/v1/ios_data_feed.json are deprecated and will be removed soon.

Osquery

Use Osquery with the MacAdmins Open Source (MAOS) Osquery Extension and the new SOFA tables to monitor unpatched CVEs on macOS. By leveraging the `sofa_unpatched_cves` and `sofa_info` tables, you can identify vulnerabilities and pat levels not addressed by current system updates across your fleet. This use case en security monitoring by providing insights into unpatched and actively exploited ensuring systems are kept up to date and secure.

For more details, visit the original blog post about SOFA and MacAdmi

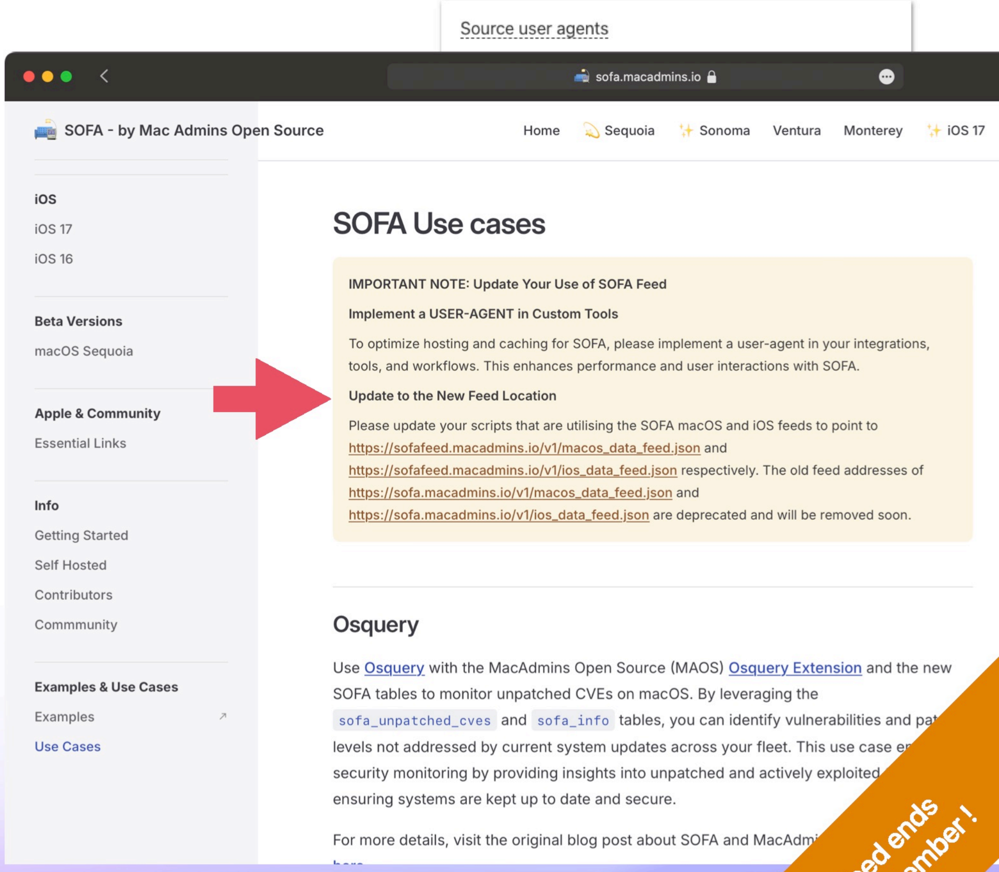
Old feed ends on 2 September !

Self-Hosting & Future Directions

Community vs. Self-hosted - why ?

Implement a USER-AGENT in Custom Tools

Update to the New Feed Location



SOFA Use cases

IMPORTANT NOTE: Update Your Use of SOFA Feed

Implement a USER-AGENT in Custom Tools

To optimize hosting and caching for SOFA, please implement a user-agent in your integrations, tools, and workflows. This enhances performance and user interactions with SOFA.

Update to the New Feed Location

Please update your scripts that are utilising the SOFA macOS and iOS feeds to point to https://sofafeed.macadmins.io/v1/macos_data_feed.json and https://sofafeed.macadmins.io/v1/ios_data_feed.json respectively. The old feed addresses of https://sofa.macadmins.io/v1/macos_data_feed.json and https://sofa.macadmins.io/v1/ios_data_feed.json are deprecated and will be removed soon.

Osquery

Use Osquery with the MacAdmins Open Source (MAOS) Osquery Extension and the new SOFA tables to monitor unpatched CVEs on macOS. By leveraging the `sofa_unpatched_cves` and `sofa_info` tables, you can identify vulnerabilities and pat levels not addressed by current system updates across your fleet. This use case e security monitoring by providing insights into unpatched and actively exploited ensuring systems are kept up to date and secure.

For more details, visit the original blog post about SOFA and MacAdmi here

Old feed ends on 2 September !

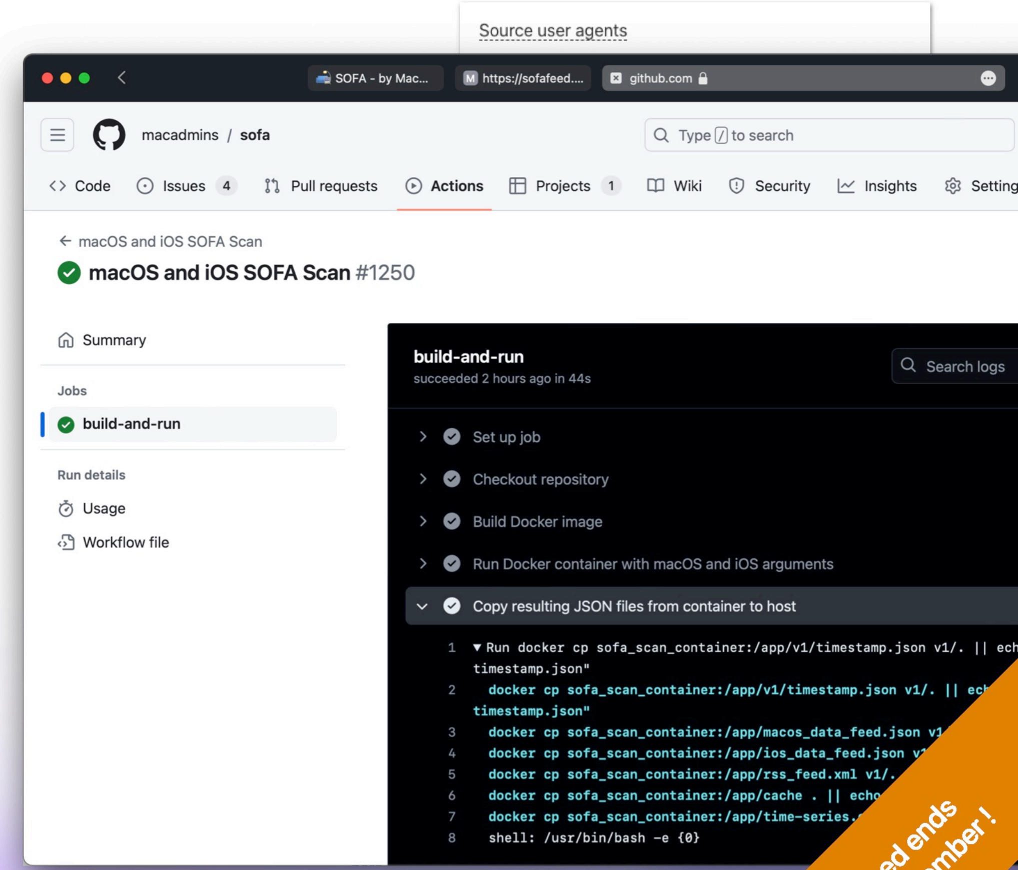
Self-Hosting & Future Directions

Community vs. Self-hosted - why ?

Implement a USER-AGENT in Custom Tools

Update to the New Feed Location

See documentation on self-hosting …



Source user agents

SOFA - by Mac… | https://sofafeed.… | github.com

macadmins / sofa

Type / to search

Code | Issues 4 | Pull requests | Actions | Projects 1 | Wiki | Security | Insights | Setting

← macOS and iOS SOFA Scan

macOS and iOS SOFA Scan #1250

Summary

Jobs

build-and-run

Run details

Usage

Workflow file

build-and-run

succeeded 2 hours ago in 44s

Search logs

- Set up job
- Checkout repository
- Build Docker image
- Run Docker container with macOS and iOS arguments
- Copy resulting JSON files from container to host

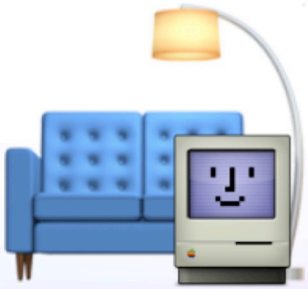
```
▼ Run docker cp sofa_scan_container:/app/v1/timestamp.json v1/. || ech
timestamp.json"
  docker cp sofa_scan_container:/app/v1/timestamp.json v1/. || ech
timestamp.json"
  docker cp sofa_scan_container:/app/macos_data_feed.json v1
  docker cp sofa_scan_container:/app/ios_data_feed.json v1
  docker cp sofa_scan_container:/app/rss_feed.xml v1/.
  docker cp sofa_scan_container:/app/cache . || echo
  docker cp sofa_scan_container:/app/time-series.
  shell: /usr/bin/bash -e {0}
```

Old feed ends on 2 September !

DEMO - Self Hosted

Basic GitHub WebUI

Q & A



Thank you !

https://sofa.macadmins.io