FINITE STATE

Project Risk Summary Report

Project Name:
Reachability Sample

Version:
1.0

Organization:
Fs-Yolo

Published: **2025-07-25**

INTRODUCTION

About Finite State

Finite State was founded to protect the devices that power our modern lives by illuminating the vulnerabilities and threats within their complex software supply chains. We recognize that supply chain security is the #1 problem in cyber security today. Global software supply chains are opaque and complicated, involving countless developers, vendors, and components. Malicious actors exploit supply chain vulnerabilities to gain access to the networks that power our critical infrastructure and can carry out potentially devastating attacks.

Finite State defends these critical devices, networks, and supply chains by leveraging massive data analysis of device firmware and software to provide transparency to device manufacturers and their customers - enabling them to understand and mitigate their risks before they are compromised.

This report by Finite State provides comprehensive security analysis of your product and its firmware. Combined, this provides insight into the firmware and its vulnerabilities to help protect and secure your mission critical products.

Confidentiality and Privacy

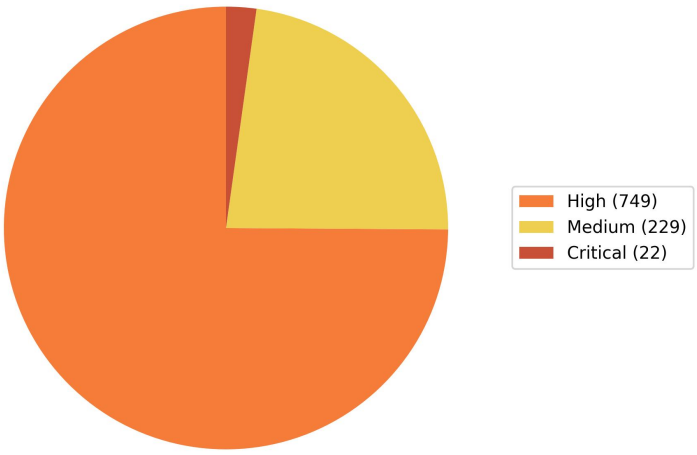
Finite State, Inc., ("Finite State," "we," or "us") respects the privacy of our customers, business partners, event attendees, job applicants, and visitors to Finite State websites ("Sites"). We recognize the need for appropriate protections and management of personal information that is shared with and provided to Finite State. Finite State has developed this Privacy Policy to assist you to understand what personal information Finite State collects and how that personal information is used. It also describes your choices regarding the use, access and correction of your personal information. This Privacy Policy applies to Sites operated by Finite State such as www.finitestate.io and other webpages in which we post and directly link to this policy.

EXECUTIVE SUMMARY

This report provides a comprehensive security assessment of **Reachability Sample** version **1.0**. The analysis identified **186 software components** and **2,677 security findings** across the project.

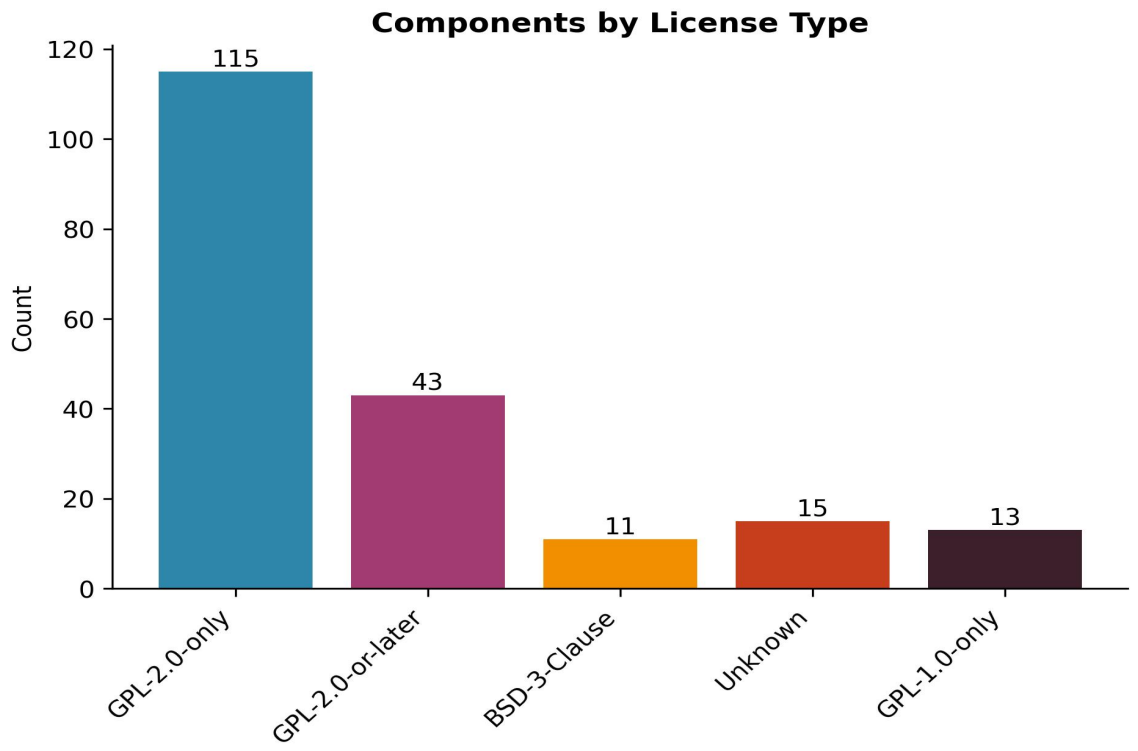
186	2677	22	749	229	0
Total Components	Total Findings	Critical	High	Medium	Low

RISK OVERVIEW



COMPONENT ANALYSIS

The analysis identified **186 software components** within the project. These components have been analyzed for licensing and security vulnerabilities.



COMPONENT RISK ANALYSIS

The following components have been identified as the highest risk based on their vulnerability counts, severity levels, and policy compliance issues. These components should be prioritized for remediation.

Component	Version	Critical	High	Medium	Low	Violations	Warnings
Linux	3.10.108	22	749	1818	81	72	1870
cls_flow		0	0	0	0	0	0
nls_cp936		0	0	0	0	0	0
krng		0	0	0	0	0	0
ip6table_nat		0	0	0	0	0	0
pcompress		0	0	0	0	0	0
ip6table_raw		0	0	0	0	0	0
crc32		0	0	0	0	0	0
authenc		0	0	0	0	0	0
crypto_blkcipher		0	0	0	0	0	0

REACHABILITY ANALYSIS

The analysis identified **89 reachable findings** and **1828 unreachable findings**. Reachable findings indicate vulnerabilities that are potentially accessible in the codebase, while unreachable findings are not accessible.

Top 100

#	Finding ID	Component	Severity	Result	Score	Risk
1	CVE-2022-27666	Linux	High	Reachable	100	7.8
2	CVE-2024-35896	Linux	High	Reachable	100	7.1
3	CVE-2025-21764	Linux	High	Reachable	50	7.8
4	CVE-2025-21760	Linux	High	Reachable	50	7.8
5	CVE-2025-21759	Linux	High	Reachable	50	7.8
6	CVE-2024-56606	Linux	High	Reachable	50	7.8
7	CVE-2024-56600	Linux	High	Reachable	50	7.8
8	CVE-2024-47742	Linux	High	Reachable	50	7.8
9	CVE-2024-46744	Linux	High	Reachable	50	7.8
10	CVE-2024-44987	Linux	High	Reachable	50	7.8
11	CVE-2024-26882	Linux	High	Reachable	50	7.8
12	CVE-2021-47634	Linux	High	Reachable	50	7.8
13	CVE-2021-47103	Linux	High	Reachable	50	7.8
14	CVE-2021-22555	Linux	High	Reachable	50	7.8
15	CVE-2017-9077	Linux	High	Reachable	50	7.8
16	CVE-2017-18509	Linux	High	Reachable	50	7.8
17	CVE-2017-17806	Linux	High	Reachable	50	7.8
18	CVE-2017-16939	Linux	High	Reachable	50	7.8
19	CVE-2017-15649	Linux	High	Reachable	50	7.8
20	CVE-2016-9755	Linux	High	Reachable	50	7.8
21	CVE-2023-52340	Linux	High	Reachable	50	7.5
22	CVE-2022-36946	Linux	High	Reachable	50	7.5
23	CVE-2025-21920	Linux	High	Reachable	50	7.1
24	CVE-2024-50035	Linux	High	Reachable	50	7.1
25	CVE-2024-50033	Linux	High	Reachable	50	7.1
26	CVE-2024-38538	Linux	High	Reachable	50	7.1
27	CVE-2024-26982	Linux	High	Reachable	50	7.1
28	CVE-2022-1353	Linux	High	Reachable	50	7.1

29	CVE-2023-52578	Linux	High	Reachable	50	7.0
30	CVE-2024-50038	Linux	Medium	Reachable	300	5.5
31	CVE-2018-1065	Linux	Medium	Reachable	100	4.7
32	CVE-2024-42229	Linux	Medium	Reachable	100	4.1
33	CVE-2013-4470	Linux	Medium	Reachable	50	6.9
34	CVE-2021-0920	Linux	Medium	Reachable	50	6.4
35	CVE-2013-4312	Linux	Medium	Reachable	50	6.2
36	CVE-2014-2309	Linux	Medium	Reachable	50	6.1
37	CVE-2013-4387	Linux	Medium	Reachable	50	6.1
38	CVE-2020-25211	Linux	Medium	Reachable	50	6.0
39	CVE-2025-21922	Linux	Medium	Reachable	50	5.5
40	CVE-2024-57996	Linux	Medium	Reachable	50	5.5
41	CVE-2024-50304	Linux	Medium	Reachable	50	5.5
42	CVE-2024-50142	Linux	Medium	Reachable	50	5.5
43	CVE-2024-49940	Linux	Medium	Reachable	50	5.5
44	CVE-2024-40960	Linux	Medium	Reachable	50	5.5
45	CVE-2024-40959	Linux	Medium	Reachable	50	5.5
46	CVE-2024-36902	Linux	Medium	Reachable	50	5.5
47	CVE-2024-36901	Linux	Medium	Reachable	50	5.5
48	CVE-2024-36286	Linux	Medium	Reachable	50	5.5
49	CVE-2024-35969	Linux	Medium	Reachable	50	5.5
50	CVE-2024-35945	Linux	Medium	Reachable	50	5.5
51	CVE-2024-26973	Linux	Medium	Reachable	50	5.5
52	CVE-2024-26675	Linux	Medium	Reachable	50	5.5
53	CVE-2024-26635	Linux	Medium	Reachable	50	5.5
54	CVE-2024-25740	Linux	Medium	Reachable	50	5.5
55	CVE-2024-25739	Linux	Medium	Reachable	50	5.5
56	CVE-2023-52449	Linux	Medium	Reachable	50	5.5
57	CVE-2023-0394	Linux	Medium	Reachable	50	5.5
58	CVE-2022-49728	Linux	Medium	Reachable	50	5.5
59	CVE-2022-49021	Linux	Medium	Reachable	50	5.5
60	CVE-2022-48911	Linux	Medium	Reachable	50	5.5
61	CVE-2022-48839	Linux	Medium	Reachable	50	5.5
62	CVE-2022-3543	Linux	Medium	Reachable	50	5.5
63	CVE-2021-47258	Linux	Medium	Reachable	50	5.5
64	CVE-2021-47182	Linux	Medium	Reachable	50	5.5

65	CVE-2021-47146	Linux	Medium	Reachable	50	5.5
66	CVE-2021-29650	Linux	Medium	Reachable	50	5.5
67	CVE-2019-20812	Linux	Medium	Reachable	50	5.5
68	CVE-2019-20422	Linux	Medium	Reachable	50	5.5
69	CVE-2017-9242	Linux	Medium	Reachable	50	5.5
70	CVE-2017-15116	Linux	Medium	Reachable	50	5.5
71	CVE-2016-8645	Linux	Medium	Reachable	50	5.5
72	CVE-2024-26804	Linux	Medium	Reachable	50	5.3
73	CVE-2013-7446	Linux	Medium	Reachable	50	5.3
74	CVE-2016-7917	Linux	Medium	Reachable	50	5.0
75	CVE-2015-8215	Linux	Medium	Reachable	50	5.0
76	CVE-2014-8160	Linux	Medium	Reachable	50	5.0
77	CVE-2015-7799	Linux	Medium	Reachable	50	4.9
78	CVE-2013-7270	Linux	Medium	Reachable	50	4.9
79	CVE-2013-7263	Linux	Medium	Reachable	50	4.9
80	CVE-2023-53020	Linux	Medium	Reachable	50	4.7
81	CVE-2022-49344	Linux	Medium	Reachable	50	4.7
82	CVE-2019-16994	Linux	Medium	Reachable	50	4.7
83	CVE-2013-6431	Linux	Medium	Reachable	50	4.7
84	CVE-2023-7192	Linux	Medium	Reachable	50	4.4
85	CVE-2022-0494	Linux	Medium	Reachable	50	4.4
86	CVE-2020-15437	Linux	Medium	Reachable	50	4.4
87	CVE-2019-15666	Linux	Medium	Reachable	50	4.4
88	CVE-2021-38209	Linux	Low	Reachable	50	3.3
89	CVE-2015-2922	Linux	Low	Reachable	50	3.3
90	CVE-2021-47548	Linux	Critical	Unreachable	-50	9.8
91	CVE-2021-47378	Linux	Critical	Unreachable	-50	9.8
92	CVE-2019-18814	Linux	Critical	Unreachable	-50	9.8
93	CVE-2019-17133	Linux	Critical	Unreachable	-50	9.8
94	CVE-2019-16746	Linux	Critical	Unreachable	-50	9.8
95	CVE-2019-15505	Linux	Critical	Unreachable	-50	9.8
96	CVE-2017-7895	Linux	Critical	Unreachable	-50	9.8
97	CVE-2017-18174	Linux	Critical	Unreachable	-50	9.8
98	CVE-2023-52832	Linux	Critical	Unreachable	-50	9.1
99	CVE-2023-52735	Linux	Critical	Unreachable	-50	9.1
100	CVE-2021-47354	Linux	Critical	Unreachable	-50	9.1

EXPLOITS SUMMARY

The analysis found **422 findings with exploit information**. These have been categorized by exploit maturity and availability.

Exploited By Ransomware	1
Exploited By Botnet	1
Exploited By Threat Actors	7
In KEV	5
Reported in the Wild	9
Commercial Exploit	8
Weaponized	19
PoC	363

TOP SECURITY RISKS

CVE ID	Severity	Risk Score	EPSS Percentile	Component
CVE-2021-47548	Critical	9.8	17.5%	Linux
CVE-2021-47378	Critical	9.8	21.8%	Linux
CVE-2021-3773	Critical	9.8	79.6%	Linux
CVE-2019-18814	Critical	9.8	65.2%	Linux
CVE-2019-17133	Critical	9.8	81.4%	Linux
CVE-2019-16746	Critical	9.8	85.1%	Linux
CVE-2019-15505	Critical	9.8	65.8%	Linux
CVE-2019-14897	Critical	9.8	71.1%	Linux
CVE-2019-14896	Critical	9.8	81.8%	Linux

CVE-2019-14895	Critical	9.8	78.5%	Linux

HELPFUL INFORMATION

View this resource to learn more about terms, definitions, and helpful information to understand the firmware risk report.

CORE SECURITY TERMS

Term	Definition
Risk Score	A composite risk score computed by Finite State based on multiple subcomponents and comparison to other binaries. Higher scores indicate greater risk.
Severity	Qualitative risk levels: Critical, High, Medium, Low. Used to categorize the potential impact of security findings.
CVE	Common Vulnerabilities and Exposures - publicly known security vulnerabilities documented in the National Vulnerability Database (NVD).
EPSS Percentile	Exploit Prediction Scoring System percentile (0-100) indicating the likelihood of exploitation compared to all known vulnerabilities. Higher percentiles indicate greater exploitation probability.

COMPONENT AND SOFTWARE TERMS

Term	Definition
Software Bill of Materials (SBOM)	A list of software components found within firmware, including open-source and proprietary components used to assemble the software.
Component	A software component or library that is part of the analyzed firmware or software package.
License	The software license under which a component is distributed, affecting legal and compliance considerations.

EXPLOIT AND THREAT INTELLIGENCE TERMS

Term	Definition
Exploited By Ransomware	Indicates active, high-impact exploitation often resulting in major business disruption.
Exploited By Botnet	Part of mass exploitation campaigns, indicating wide exposure risk.
Exploited By Threat Actors	Known use by real adversaries; strong signal of risk.
In KEV	Listed in CISA Known Exploited Vulnerabilities Catalog based on past exploitation; prioritization recommended by authoritative sources.
Reported in the Wild	Observed being used in attacks, but attribution or scope may be less clear than above.
Commercial Exploit	Available to buyers (e.g., via private brokers); implies advanced threat use.
Weaponized	Packaged in a ready-to-use exploit format (e.g., part of exploit kits or frameworks).
PoC (Proof of Concept)	A working exploit is available, but not necessarily used yet. Still high risk, especially if easy to use.

SECURITY ANALYSIS TERMS

Term	Definition
Credentials	User accounts and credentials found in firmware that can indicate potential backdoors or unauthorized access points.
Crypto Material	Private keys and authorized key files that can indicate backdoors allowing unintended device access.
Exploit Mitigations	Modern software compiler safety features designed to prevent common exploit methods like buffer overflows.

Unsafe Function Calls	Legacy functions (like strcpy) in C that are unsafe and expose binaries to risks like buffer overflow. The platform detects these calls and uses their ratio to total function calls to percentile rank firmware.
Potential Memory Corruptions	Binaries with the highest potential for buffer overflows and other memory-related attacks.
Code Analysis	Static analysis results of source code, identifying security issues like invoking shell commands or command injections. Currently analyzes Python source code.

PROJECT AND VERSION TERMS

Term	Definition
Project	A software project or product being analyzed for security vulnerabilities.
Version	A specific version or release of a project being analyzed.
Finding	A security vulnerability or issue identified during the analysis process.
Violations	Policy violations related to security findings that may require immediate attention.
Warnings	Policy warnings associated with findings that should be reviewed and addressed.