

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Protecting Against National Security)	WC Docket No. 18-89
Threats to the Communications Supply)	
Chain Through FCC Programs)	
)	

**WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD.,
AND HUAWEI TECHNOLOGIES USA, INC.**

Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc. (collectively, “Huawei”), by their undersigned counsel, submit this *ex parte* presentation to the Federal Communications Commission (“FCC” or “Commission”) to supplement the record in the above-captioned docket. In particular, Huawei responds to the *Draft Report and Order*’s citation to a 2019 report by Finite State (the “Finite State Report”) which purports to assess the security of Huawei’s products and services.¹

Huawei has publicly responded to the Finite State Report, highlighting significant flaws in the methodology used and factual errors that undercut the Report’s conclusions. Attached as **Exhibit 1** is a statement released by Huawei regarding the Finite State Report, and a technical analysis of the Finite State Report performed by Huawei’s Product Security Incident Response Team (“PSIRT”) is attached as **Exhibit 2**.

¹ See *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, para. 51 (circulated Oct. 29, 2019) (“*Draft Report and Order*”) (citing Finite State, Finite State Supply Chain Assessment at 3 (2019), <https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf>) (“*Finite State Report*”).

In summary, the Finite State Report is replete with basic errors. Although it asserts otherwise, the Finite State Report evaluated old versions of Huawei's products and identified issues that had been fixed in updated versions of these products. The Finite State Report bases some of its conclusions about potential backdoors on the assumption that Huawei uses standard Linux-based authentication,² but it does not. More generally, Finite State failed to follow general practices of responsible security testing companies, which typically involves dialogue between the security company and vendor about alleged vulnerabilities to help ensure a complete and accurate picture of security vulnerabilities. The Report also contains no explanation of how Finite State selected the vendors it used for purposes of comparison in its study, why it ignored the vendor who holds the largest market share of the global enterprise network, or why it tested almost all of the hundreds of Huawei enterprise network products, but only one product each of Juniper and Arista without disclosing the versions assessed. The Finite State Report also includes a background section that includes unsupported and erroneous assertions. For example, it cites erroneous reporting suggesting that Vodafone found an alleged "backdoor" in Huawei's equipment in Italy.³ But Vodafone itself has explained that the alleged backdoor was no backdoor at all and the issue was resolved in 2011 and 2012.⁴

² See *Finite State Report*, at 27.

³ See *Finite State Report*, at 5 (asserting, incorrectly, that Vodafone had found vulnerabilities associated with Huawei equipment).

⁴ See "Vodafone denies Huawei Italy security risk," BBC News, (Apr. 30, 2019), <https://www.bbc.com/news/business-48103430> (noting "In a statement, Vodafone said: 'The issues in Italy identified in the Bloomberg story were all resolved and date back to 2011 and 2012[]'" and that Vodafone has "'no evidence of any unauthorised [sic] access. This was nothing more than a failure to remove a diagnostic function after development.'").

The *Draft Report and Order* is bereft of *any* assessment of the methodology or the accuracy of the assertions made in the Finite State Report and simply accepts the Report's conclusions at face value. That is untenable in light of the many easily discoverable errors in the Finite State Report. The Commission's reliance on the Finite State Report to support its conclusion that Huawei poses national security risk to communications networks in the United States would be irrational, arbitrary, and capricious. As Huawei has extensively advocated in this proceeding and elsewhere, a risk-based security approach, including the use of independent, third-party testing of products from all equipment vendors using internationally recognized standards, will do far more to protect communications infrastructure in the United States and elsewhere from cybersecurity vulnerabilities than banning the use of equipment by specific vendors.

Respectfully submitted,

/s/ Andrew D. Lipman

Andrew D. Lipman
Russell M. Blau
David B. Salmons

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

*Counsel to Huawei Technologies Co., Ltd.,
and Huawei Technologies USA, Inc.*

October 31, 2019

EXHIBIT LIST

Exhibit 1: “Finite State Report Fails to Tell the Whole Story”

Exhibit 2: Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment

Exhibit 1

“Finite State Report Fails to Tell the Whole Story”



Finite State report fails to tell the whole story

Huawei is serious about cyber security and welcomes any objective input that makes our technology more secure. This includes analyses that publicly disclose any weaknesses our products may have.

On June 25, a US cyber security firm called [Finite State released a report](#) saying Huawei products were more vulnerable than equipment made by some of our competitors. We have a Product Security Incident Response Team ([PSIRT](#)) that discloses vulnerabilities in our products when we find them. PSIRT and our engineers published an [in-depth response](#) to the technical points of Finite State's analysis.

The Finite State report is a preliminary assessment, very much like the ones Huawei (and every vendor of network equipment) conducts to test the integrity of our products. As a preliminary assessment, it does not tell the whole story.

Our initial review suggests that the data cited in their report, and the testing methods they used, would not identify significant vulnerabilities in Huawei's gear.

First, many of the products critiqued are for enterprise markets, with some data center switches for the carrier market. None of the Huawei products tested by Finite State will be deployed for 5G RAN or Core in telecommunications networks. (Products made by Cisco, the largest provider of gear for the enterprise market, were not tested.)

Second, Finite State used something called a binary image analysis tool. The tool is suitable for certain narrow security applications but cannot provide a complete and accurate picture of security vulnerabilities in the products tested.

Third, Finite State specializes in security for the Internet of Things (IoT) and may not fully understand how telecommunications equipment is deployed. For example, an important fact not referenced in the report is that after installation, default settings are zeroed out, providing network operators with secure control over their equipment. Equipment vendors also work closely with operators to address potential vulnerabilities, such as those that might be disclosed using a tool like the one Finite State used for this study.

Fourth, Finite State tested older versions of Huawei software, which might not have contained important security patches issued later. It is not clear why Finite State chose older versions when newer ones were available. We don't know how Finite State obtained the software they used, and we don't know which distribution channel they used as a source.

Finally, and significantly, Finite State did not give Huawei a chance to review its analysis before publication. Normally, firms that conduct independent analysis strive to present neutral, unbiased research; accordingly, they check any findings with the affected vendors before going public. Finite State's failure to do that raises questions about their motivation in releasing the report. More importantly, the report lacks important insights that could have been provided to make it more complete, and more accurate.

The inclusion of extraneous, negative information about Huawei also suggests that objectivity was not a major consideration. For example, several pages outline "Key security concerns" about Huawei, setting a negative tone at the outset and suggesting a presumption that Huawei products are flawed.

Finite State also cited a Bloomberg story which incorrectly reported that Vodafone had found "backdoors" in Huawei's network gear in Italy. Vodafone quickly corrected the report, explaining that what Bloomberg had mistakenly called a backdoor was, in fact, [part of a routine diagnostic function](#) commonly used in the telecommunications industry. Yet, although Vodafone published the official statement in April, Finite State's June report still cited the erroneous Bloomberg story and did not mention the correction.

Huawei is committed to securing critical network infrastructure. We work with independent researchers and testing firms worldwide to find, and fix, vulnerabilities that might compromise security. Because we are headquartered in China, we are probably the most frequently, most thoroughly tested technology provider in the world. Even so, no one has ever found any evidence of cyber security wrongdoing in our equipment. Because of the important insights gained from expert, independent reviews of our technology, we will spend US\$2 billion in the coming years to revamp our software engineering processes and improve our software quality and security.

Again, we have no problem letting people pick apart our software; in fact, we have [facilities dedicated to doing just that](#). But the testing methodology employed by Finite State is not, by itself, sufficient to provide what the global community needs: an objective, transparent method of testing the products sold by technology providers based on uniform global standards.

That said, we would welcome the opportunity to speak with Finite State about their findings, in hopes of gaining insights that can help us improve our practices and further inform our software engineering revamp.

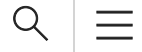
Finite State's report implicitly supports Huawei's longstanding call for independent, third-party testing of products from all equipment vendors, using internationally recognized standards. Such an approach would help move important conversations about cyber security away from the realm of politics, toward the domain of science, engineering, and facts. And that would help make cyberspace a safer place.

July 9, 2019

Huawei Technologies Co., Ltd.

Exhibit 2

Huawei PSIRT: Technical Analysis Report Regarding
Finite State Supply Chain Assessment



[Home](#) > [PSIRT](#) > [Security Notices](#)

Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment

Last Release Date: Jul 03, 2019

At Huawei, we welcome collaboration with cyber security researchers and independent testing of our products and solutions. We have a long-established Product Security Incident Response Team (PSIRT) that manages the collection, investigation, internal coordination and responsible disclosure of security vulnerability information related to Huawei products. Once a vulnerability has been confirmed, PSIRT promptly conveys the information to the teams responsible for the affected products, and then actively tracks the progress to resolution.

Huawei has built and implemented a multi-tiered end-to-end cyber security evaluation process to ensure that our products are reviewed for potential security issues from product concept, design, development, and right throughout to deployment and maintenance in our customers' networks around the world.

On June 26, 2019, U.S.-based Finite State publicly disclosed the *Supply Chain Assessment* report about Huawei on its official website. In this report, Finite State describes its use of a static analysis tool for firmware images (binary software packages) to analyze more than 500 Huawei enterprise network products and the comparison analysis between Huawei CE12800, Juniper EX4650, and Arista 7280R, with conclusions that Huawei products have poorer security and potential backdoors.



We were surprised and disappointed by the unconventional approach of Finite State. We cannot determine whether Finite State obtained the software from legitimate channels or guarantee its integrity, nor has Huawei ever received any communication requests from Finite State. They made no contact with Huawei to assist them in their understanding and refused to provide a copy of their analysis before it was published. Sadly, this means what has been published lacks the insight, integrity and accuracy we would normally expect from a professional, serious and capable organization.

Due to the approach Finite State has taken and the weakness of their tools and methodology, the results are at best suspect and at worst just inaccurate. This could have been avoided by collaborating rather than taking a political stance on security.

We are unsure of the objectives of the CEO Matt Wyckhouse and Finite State overall and why they did not select the market leader Cisco for comparison, or indeed why they evaluated old versions of Huawei products and identified issues that had been fixed in new versions.

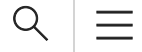
Whilst Finite State has had many months to undertake their flawed analysis, over the last few days Huawei PSIRT has investigated the issues mentioned in the report immediately after the report was published. We believe that the approach used by Finite State has serious operational and technical defects, the tests lack neutrality, and the report contains material inaccuracies.

1 Finite State's Test Process and Report Development Approach Are Contrary to General Practices of Responsible Security Testing Companies

Responsible disclosure of security issues or vulnerabilities is widely recognized and practiced by the industry. Typically, security research organizations or researchers deliver identified issues and potential vulnerabilities to vendors, and vendors then confirm whether they are defects or vulnerabilities and carry out coordinated handling. Finite State simply used a tool to scan raw binaries and then conducted simple partial reverse analysis of some potential issues to reach their conclusions. Finite State has not used vulnerability exploitation in real-world products to verify the analysis, nor has the analysis been confirmed by Huawei product R&D. Binary vulnerability scanning tools are generally used for auxiliary analysis because their error rate can reach up to over 90%. Thus, Finite State's conclusions are drawn in a hasty manner and are inaccurate. Although Finite State mentions the limitations of the tool it has developed and used, for example, the tool does not support analysis in context, and vulnerabilities are based on file names and version information, Finite State has overestimated the sophistication and accuracy of its tool. As we demonstrate in Appendix, independent analysts do not rank Finite State tools as market leaders in any dimension.



Finite State made a hasty and unprofessional decision to deliver the assessment report to the media and government authorities, without providing it to Huawei beforehand, nor have the issues been confirmed by Huawei. This practice is contrary to best practice or even basic common sense in terms of responsible security organizations in the industry. A fair security technology organization shall remain neutral and express opinions from the perspective of technical security.



Finite State's assessment report repeatedly mentions potential backdoors in Huawei products in an emotional and overstated way. Any security company that claimed it has discovered many backdoors and unfixed serious vulnerabilities by tool-based scanning and without verifying the products or even having any context or knowledge of the products, their architecture and environment, cannot be taken seriously.

2 Assessment Report Gives No Explanation About the Selection of Vendors, Products and Versions for Comparison, and Selective Tests Have Been Conducted

The assessment report does not explain why products of Huawei, Juniper, and Arista were used as test samples but Cisco, another company who holds the largest market share of the global enterprise network. Why weren't Cisco products evaluated? Finite State tested almost all of the hundreds of Huawei enterprise network products, but only one product of Juniper and Arista without disclosing their versions. According to the report, it states that the latest versions of Huawei products are used, however, all versions mentioned in the report are actually old versions. For example, AR1200 V200R007C00SPCc00 released in 2017 was used. However, the updated versions released in 2018 and 2019, such as V200R009 and V200R010, are available on Huawei's technical support website. Moreover, AR3600 V200R007C00SPCb00 released in 2016 was used, but the updated versions released in 2018 and 2019, such as V200R008 and V200R009, are also available on Huawei's technical support website.

We believe selective tests have been conducted, with intentionally selected versions and comparison objects to achieve the "expected" results for Finite State or those that funded this "research".

3 Finite State's Conclusions Are False Through Our Investigation and Analysis

Regarding Finite State's conclusions, Huawei products have backdoors and many vulnerabilities or even serious vulnerabilities left unfixed, Huawei PSIRT and R&D have undertaken a detailed analysis and reached the following conclusions after verification.

3.1 Analysis of Suspected Backdoors

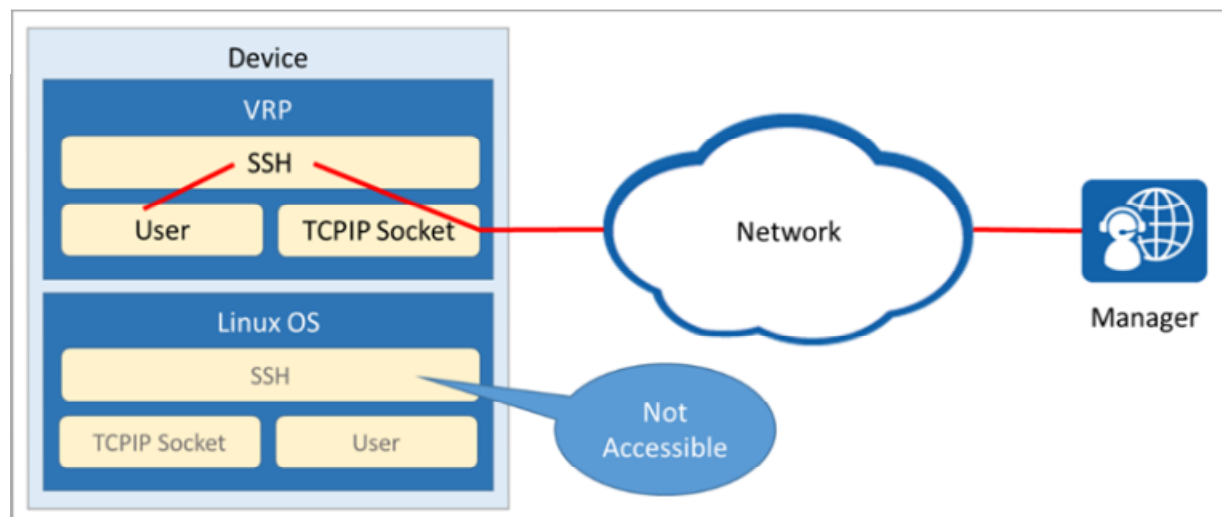


Many suspected backdoor conclusions drawn by Finite State are based on the prerequisite that Huawei is using standard Linux-based authentication. However, this prerequisite is incorrect and thereby the stated conclusions are wrong.

3.1.1 Analysis of Undocumented and Hard-coded Credentials

The report shows that *huawei*, *python*, and *root* accounts are potential privilege escalation backdoors. In fact, the three accounts identified cannot be used for unauthorized privilege escalation. The analysis is as follows:

Huawei AR products use only basic functions of Linux, such as task scheduling. Other functions, namely, user management, remote access control, and TCP/IP protocol stack, are taken over by Huawei Versatile Routing Platform (VRP). This design can better meet application requirements of products. Many telecommunications companies in the industry also use the similar design pattern, as shown in the following figure.



VRP taking over remote user access

The *root* account is used to start the VRP process. It is used internally and invisible externally. The *python* and *huawei* accounts are used by VRP users with the highest privileges to create VMs and install third-party applications. These accounts are invisible externally. The three accounts are protected from being exploited for remote device access and do not compromise system security.

It is true that the `sudo` configuration and `sbin/inssmod` commands mentioned in the report may be exploited for privilege escalation. Huawei PSIRT has confirmed that this is a known and fixed vulnerability. The device administrator shall be assigned the least privilege to reduce risks. Huawei has eliminated the risk in V300R003C00SPC500



(released in August 2018) by using the program code to implement related management functions.



In addition, the *huawei*, *python*, and *root* accounts are documented in [Command Reference](#) (2018)

3.1.2 Analysis of Default Hard-coded Cryptographic Keys

As described in the report, the `authorized_keys` and similar files are engineering tools used during the development process. The E9000 and CE12800 R&D engineers use SSH of the Linux OS to facilitate debugging, and leave the key files in the firmware.

As illustrated in section 3.1.1 "Analysis of Undocumented and Hard-coded Credentials", Huawei datacom products use the basic functions of Linux. Remote access control and TCP/IP protocol stack are taken over by the VRP. In official versions, the debugging function is disabled, and external users cannot access SSH of the Linux OS. Therefore, these key files do not cause any potential unauthorized access. These key files will be deleted in the version to be released in September 2019.

The report shows the presence of an `authorized_keys` file for the superuser account on the firmware image of SmartAX MA5800, but the SSH code has been deleted from the released versions, and therefore no security risks exist.

3.2 Analysis of Known Vulnerabilities Not Fixed

The report describes the use of outdated components and we agree with this analysis and have already announced substantial upgrades to enhance our products in this regard... However, the presence of outdated components does not necessarily mean the presence of security issues.

The known vulnerability analysis method SCA mentioned in the report is used to assess known vulnerabilities by open-source software name and version number. This method is defective for embedded devices because of the following causes:

- (1) Code related to open-source component vulnerabilities is not compiled into the firmware.
- (2) For some open-source software, after a vulnerability is detected, the source code patch will be preferentially released to fix the vulnerability. Then a formal fix version is planned. This process may take a long time depending on the open source community approach. To fix the vulnerability as soon as possible, telecom vendors usually incorporate the fixed source code. However, the version number of the open-source software used in the product firmware is still the old version number.




(3) The method of fixing vulnerabilities using binaries is similar to (2). The version number of the open-source software remains unchanged.

(4) The vulnerable code in the open-source component is included in the firm-ware, but the corresponding functional module is not used.

After analyzing the 10 well-known vulnerabilities reported in AR3600 V200R007C00SPCb00, we find that 6 vulnerabilities cause no impact, 2 are fixed, and 2 are of low risks. The details are as follows:

Vulnerability Name	Component	CVE ID	Analysis Result
DROWN	OpenSSL	CVE-2016-0800	This vulnerability affects only SSL V2. The earliest version supported by products is SSL V3.
FREAK	OpenSSL	CVE-2015-0204	The vulnerability is fixed by incorporating the fixed code, but the OpenSSL version remains unchanged.
POODLE	OpenSSL	CVE-2014-3566	The vulnerability is fixed by incorporating the fixed code, but the OpenSSL version remains unchanged.
Heartbleed	OpenSSL	CVE-2014-0160	The vulnerable openssl1.0.1e is used on cards, but the OpenSSL function on the cards is not used.
Quadrouter	Linux Kernel	CVE-2016-2059	The kernel is tailored, and the vulnerable code is not included in the product package.
Quadrouter	Linux Kernel	CVE-2016-5340	The kernel is tailored, and the vulnerable code is not included in the product package.
Linux Kernel	Linux Kernel	CVE-2016-5696	This vulnerability is present in the TCP/IP protocol stack of the Linux kernel. It is involved only when the AR3600 needs to load the system software package in boot mode (only in the case of serial port access). In other cases, this protocol stack is not used. Therefore, the security risk is low.
Linux Kernel	Linux Kernel	CVE-2016-0728	The kernel is tailored, and the vulnerable code is not included in the product package.
NA	Linux Kernel	CVE-2016-10229	This vulnerability is present in the TCP/IP protocol stack of the Linux kernel. It is in-



Vulnerability Name	Component	CVE ID	Analysis Result
			involved only when the AR3600 needs to load the system software package in boot mode (only in the case of serial port access). In other cases, this protocol stack is not used. Therefore, the security risk is low.
NA	OpenSSL	CVE-2016-7055	This vulnerability is present in OpenSSL 1.0.2, 1.1.0c, and earlier versions. Products use OpenSSL 1.0.1 and therefore are not affected.

3.3 Analysis of Conclusion that Huawei Situation Is Getting Worse Drawn on An Increased Number of Publicly Known CVE Vulnerabilities

Finite State concluded on page 23 of the report that the situation of Huawei is getting worse based on an increased number of CVEs, which is unscientific.

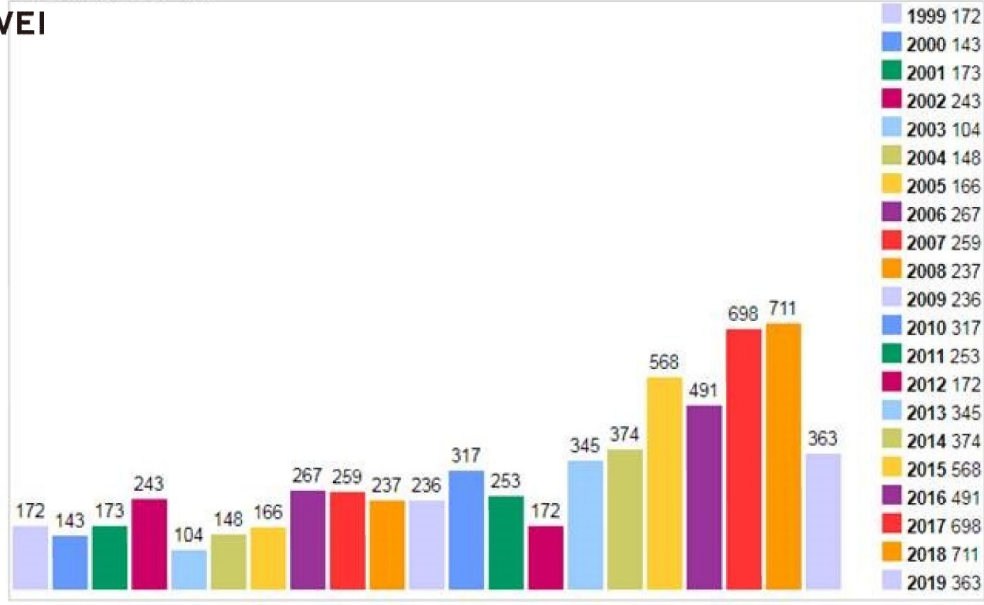
It is a basic requirement of ISO/IEC 29147:2018 Vulnerability Disclosure to disclose a vulnerability to customers and notify them of risks and mitigations after fixing the vulnerability. Huawei PSIRT is a dedicated global vulnerability response team which established Huawei's vulnerability response process based on related standards. In 2012, Huawei PSIRT established a public channel (www.huawei.com/psirt) for vulnerability disclosure.

According to the number of vulnerabilities disclosed by the NVD, the Top 5 vendors are Microsoft, Oracle, Apple, IBM, and Google.

Vulnerability trends of Microsoft show that its number of vulnerabilities remains at a certain level. This shows on one hand Microsoft's continuous investment in security and on the other hand Microsoft's responsible disclosure of vulnerabilities. In addition, Microsoft uses the bug bounty program to encourage people to discover vulnerabilities.



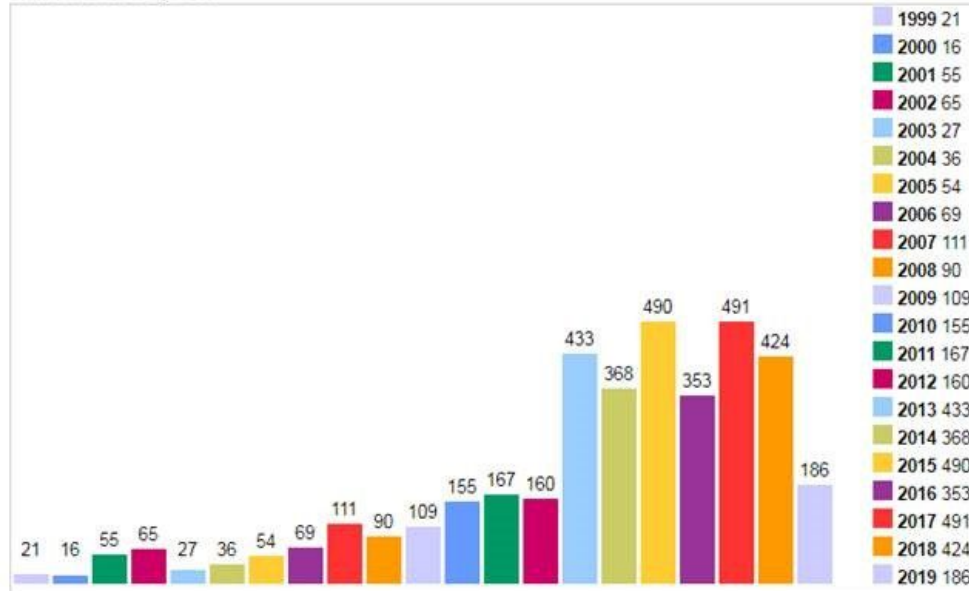
Vulnerabilities By Year



Link: <https://www.cvedetails.com/vendor/26/Microsoft.html>

Cisco also has its own vulnerability disclosure channel. The number of vulnerabilities disclosed by Cisco also remains at a certain level.

Vulnerabilities By Year



Link: <https://www.cvedetails.com/vendor/16/Cisco.html>

3.4 Secure Coding Practices

3.4.1 Safe Function Analysis

The method used in the report to analyze safe functions has the following problems, which leads to inaccurate results:



1) The assessment does not cover a large number of safe functions in Huawei products, such as *VOS_MemCpy_Safe* and *VOS_nsprintf_Safe*, which causes serious deviation in the security assessment results.

2) Inaccurate understanding of unsafe functions

(1) The report lists on page 33 some unsafe functions, including puts, memcmp, and asprintf.

(2) As a memory clearing function, memset is used within Huawei to clear the newly applied memory and arrays with a fixed length. It has a very low risk. Even Microsoft that promotes safe functions does not have the corresponding safe function.

(3) Functions such as fopen, access, system, remove, and execl must be used in code to meet service requirements. Using these functions does not necessarily lead to vulnerabilities.

3) Some functions in the report are regarded as both safe and unsafe.

(1) asprintf is listed as an unsafe function in "Top 20 Most Commonly Used Unsafe Functions" on page 34, but is listed as a safe function later in "Safe and Unsafe Function Collections" on page 36. drv_cvb_memcpy_s_impl is listed as both a safe and unsafe function in "Safe and Unsafe Function Collections" on page 36 of the report.

(2) According to "Top 20 Most Commonly Used Unsafe Functions", the author regards the execl function as unsafe but execlp, execv, execve, execvp, execl, and execvpe as safe, which is incorrect.

3.4.2 Compiler Security Option Analysis

In addition to RELRO, ASLR, DEP, and StackGuard mentioned in the report, at least three other compiler security options are important. In an embedded communications device, enabling compiler security options generally deteriorates product performance, even prevents product functions from running properly in some cases. It demonstrates the lack of maturity and competence of Finite State to comment on the enabling of compiler security options in embedded communications software from the perspective of general software only. Huawei would be happy to teach Finite State the basics of imbedded systems and global telecommunications operations that cover the globe.

Huawei has been carrying out in-depth researches on compiler security options for many years and attaches great importance to security. We will enable compiler security options as much as possible when conditions allow. As far as we know, Huawei leads the communications industry in terms of implementation in this regard.



Finite State uses the Software Composition Analysis (SCA) method in the assessment report, which is consistent with the industry. Many companies in the industry provide such an analysis service. The report of the research firm Forrester shows their SCA vendor evaluation, in which Finite State is not found. The Forrester Wave™: Software Composition Analysis, Q2 2019 link is :<https://reprints.forrester.com/#/as-sets/2/230/RES146435/reports>.

SCA Principles

Currently, the commonly used open-source software and vulnerability analysis technology SCA have two major purposes:

- 1) Identify the version and license information of the open-source software used to ensure compliant use.
- 2) Search the vulnerability library by open-source software version to obtain all vulnerabilities in the open-source software.

Source: blog of WhiteSource, a leading SCA solution provider according to Forrester

First and foremost, SCA tools generate an inventory report of all open source components in your products, including all direct and transitive dependencies. Taking inventory of open source usage is critical as it is the basis for properly managing your open source usage. After all, how can you secure or ensure compliance of something you do not know you're using?

Once all open source components have been identified, SCA tools provide information on each component. Basic information includes the open source license and whether there's a security vulnerability associated with that component.

The SCA method analyzes the firmware in the following steps:

- 1) Extract the complete hash value, partial hash value, function symbol name, file name, etc. of each binary file in the firmware as features. Identify the name and version of the open-source software referenced in the firmware based on these features.
- 2) On the basis of open-source software name and version information obtained in step 1, search the vulnerability library and obtain all vulnerabilities in the open-source software.

The SCA result is only an intermediate result and generally needs to be further confirmed with the firmware developer.



Revision History: V1.1 UPDATED Add the link of the Software Composition Analysis from Forrester



Read [our statement repudiating Finite State's report findings](#)

Read [our response to Nokia's accusations](#)



Press & Events >



[Huawei Facts](#)

[Photo Gallery](#)

[Events](#)

[Annual Reports](#)

Partners [↗](#)

[Solution Partners](#) [↗](#)

[Service Partners](#) [↗](#)

[Channel Partners](#) [↗](#)

Support

[Consumer Support](#) [↗](#)

[Carrier Support](#) [↗](#)

[Enterprise Support](#) [↗](#)

[Security Bulletins](#)

Portals

[Careers](#) [↗](#)

[Suppliers](#) [↗](#)

[Developers](#) [↗](#)

[Huawei Blog](#) [↗](#)

Others

[Huawei Cloud](#) [↗](#)

[FusionSolar Smart PV](#) [↗](#)

[Huawei Marine](#) [↗](#)

[Honor Official Site](#) [↗](#)