MONTHLY VULNERABILITY INSIGHTS
Based on Data from Secunia Research

FEBRUARY 2023

flexera™

Author: Jeroen Braak

Contents

Introduction

Welcome to our Monthly Vulnerability Insights by Flexera. This comprehensive, monthly review is based upon data from the Secunia Research team at Flexera who produces valuable advisories leveraged by users of Flexera's Software Vulnerability Research and Software Vulnerability Manager solutions.

The Secunia Research team is comprised of several security specialists who methodically test, verify and validate disclosed vulnerabilities from hundreds of sources. Since the founding of the Secunia Research team in 2002, it has been our goal to provide the most accurate and reliable source of vulnerability intelligence.

Secunia Research software vulnerability tracking process

A vulnerability is an error in software which can be exploited with a security impact and gain. Secunia Research validates, verifies and tests vulnerability information to author security advisories which provide valuable details by following consistent and standard processes which have been refined over the years.

Whenever a new vulnerability is reported, it's verified and a Secunia Advisory is published. A Secunia Advisory provides details, including description of the vulnerability, risk rating, impact, attack vector, recommended mitigation, credits, references and more, including additional details discovered during verification and testing, thus providing the information required to make appropriate decisions about how to protect systems. Click here to learn more about Secunia Advisories and their contents.

The anatomy of a Security Advisory

A security advisory is a summary of the work that Secunia Research performs to communicate standardized, validated and enriched vulnerability research on a specific software product version.

We issue Secunia Research criticality ratings and common vulnerability scoring system (CVSS) metrics after a distinct analysis in the advisories. This dual rating method allows for a much-improved means of prioritizing by criticality—delivering a review that includes product context and related security best practices.

A *rejection advisory* issued by the research team issues means we've determined it's not worthy of your attention. This advisory comes if a vendor issues an advisory acknowledging vulnerability that we don't believe to be valid—and would have a product solution we aren't recommending or exceeding already. We send that out to save you considerable time.

If someone other than the vendor issues an advisory and we don't believe to be valid, we discard it. We take that action so you don't waste your time processing inconsequential vulnerability information.

check out this infographic.

Summary

Total advisories : **709** ↑ (last month: **621**) .

February'23 has reported **709** advisories **the third highest** number of advisories since the Secunia Research Team started in 2002. *(#1 : July'20, #2: April'20)*

Important **conclusions** from this month report are:

- **February is the 3rd month** in a row to show an increase in advisories, zero-days and threats.
- **More than 61.35%** of all advisories have vulnerabilities that can be attacked from Remote.
  From remote describes vulnerabilities where the attack vector does not require access to the system nor a local network. This category covers services, which are acceptable to expose to the Internet (for example, HTTP, HTTPS, SMTP) as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.
- The Secunia Research Team reported **5 Extremely** critical advisories this month (4 last month)
- **12 Zero-Day** Advisories reported (Apple, Microsoft, WebkitGTK)
- Over **1,233** CVE's (last month : **1,590**) were covered in the **709** Advisories.
- Threat Intelligence indicates that more **Moderately Critical Vulnerabilities** are targeted by hackers.
- More than half of all advisories are disclosed by 4 vendors (**SUSE** 17%, **Ubuntu** 15%, **Red Hat** 12%, **Amazon** 11%)
- **F5 and Cisco** are contributing to more than **50%** of all Networking related Advisories.

Last month we reported that **66.45%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware , etc.) associated with them, this month the number has been **higher** to **74.19%**

Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

Software Vulnerability – and Patch Management is becoming more and more important.
Due to the ongoing Russia-Ukraine conflict , attacks on critical infrastructures in many countries are increasing.
Back in 2019 (just before Covid) patching was recommended within 30 days (or 14 days for CVSS score 7 or higher)
Right now , hackers can deploy exploits **within 1 week** and even within **24 hours** . This means that organizations need to prioritize even better to quickly patch vulnerabilities (especially the ones with threats associated with them)
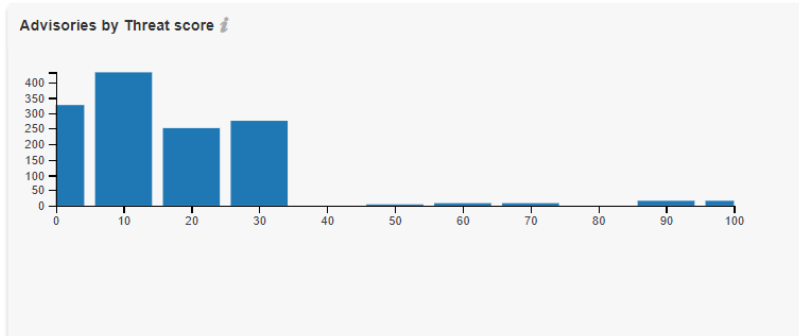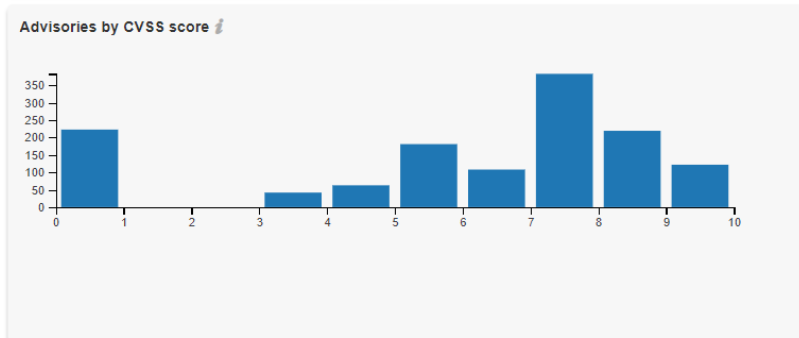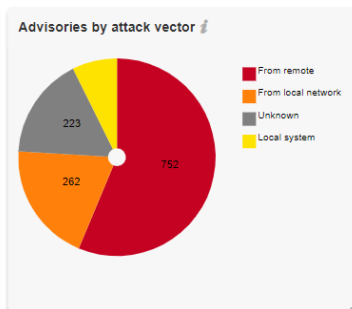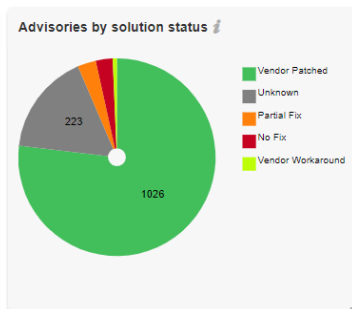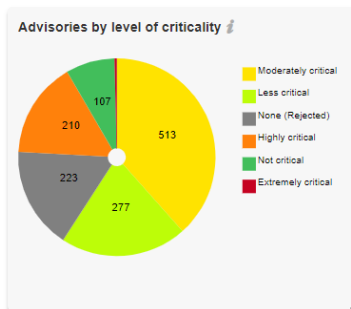
Noticeable information this month:

- Feb. 22: **VMware** on Tuesday released patches to address a critical security vulnerability affecting its **Carbon Black** App Control product tracked as CVE-2023-20858
- Feb 15: A **zero-day** vulnerability has been reported in **WebKitGTK**, which can be exploited by malicious people to compromise a vulnerable system. (CVE-2023-23529)
- Feb. 14: **Microsoft** released security updates to address **75 vulnerabilities**.
  Reported by Secunia research in 8 advisories , all of them **Zero-day** and with highest threat score of 99.
- Feb. 13: **Apple** rolled out security updates for **iOS, iPadOS, macOS, and Safari** to address a zero-day flaw that it said has been actively exploited in the wild Tracked as CVE-2023-23529.
- **CISA** added 14 vulnerabilities on the **KEV** (Known Exploited Vulnerabilities) list

Interesting sources of information:
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.bleepingcomputer.com/news/security/
- https://thehackernews.com/search/label/Vulnerability
- https://www.darkreading.com/vulnerability-management?page=1
- https://portswigger.net/daily-swig/vulnerabilities
- https://www.securityweek.com/virus-threats/vulnerabilities

Year-to-date overview

As of **February, 2023**, the year-to-date total is at **1,335** Advisories ↑ which is higher than 2022 : **1,122** YTD Advisories)

Secunia Advisories

Advisories by level of criticality

- Moderately critical
- Less critical
- None (Rejected)
- Highly critical
- Not critical
- Extremely critical

Advisories by solution status

- Vendor Patched
- Unknown
- Partial Fix
- No Fix
- Vendor Workaround

Advisories by attack vector

- From remote
- From local network
- Unknown
- Local system

Advisories by CVSS score

Advisories by Threat score

Monthly data

This month, a total of **709** ↑ (last month: **689**) advisories were reported by the Secunia Research Team.

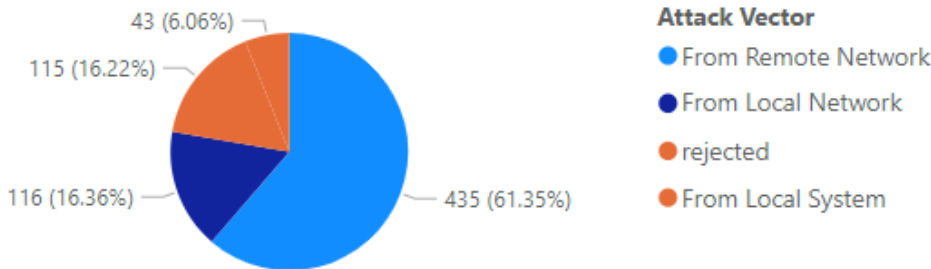| This month:	#	Change *(last month):*
Total # of advisories	709	↑ *(626)*
Unique Vendors	89	↑ *(82)*
Unique Products	366	↑ *(309)*
Unique Versions	478	↑ *(375)*
Rejected Advisories *	115	↑ *(108)*
		↑ increased ↓lower ↔ same

 * **115** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already being too privileged so that additional gain becomes neglectable). More information about rejections can be found in the rejection section.

Vulnerability information

Advisories by attack vector

43 (6.06%)
115 (16.22%)
116 (16.36%)
435 (61.35%)

Attack Vector
- From Remote Network
- From Local Network
- rejected
- From Local System

Advisories by criticality

50 (7.05%)
115 (16.22%)
126 (17.77%)
141 (19.89%)
272 (38.36%)

criticality
- Moderately Critical
- Less Critical
- Highly Critical
- Rejected
- Not Critical
- Extreme Critical
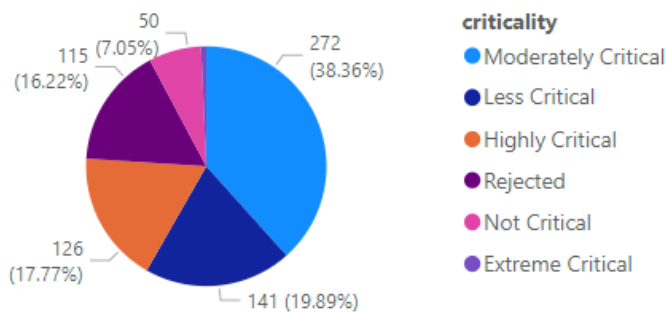
Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2023	February	1	45
2023	February	2	20
2023	February	3	14
2023	February	6	36
2023	February	7	46
2023	February	8	19
2023	February	9	31
2023	February	10	40
2023	February	13	26
2023	February	14	58
2023	February	15	77
2023	February	16	29
2023	February	17	33
2023	February	20	7
2023	February	21	47
2023	February	22	27
2023	February	23	61
2023	February	24	14
2023	February	27	33
2023	February	28	46
Total			**709**

Rejected advisories

There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.
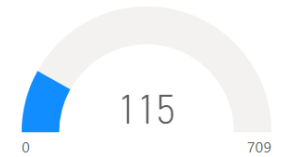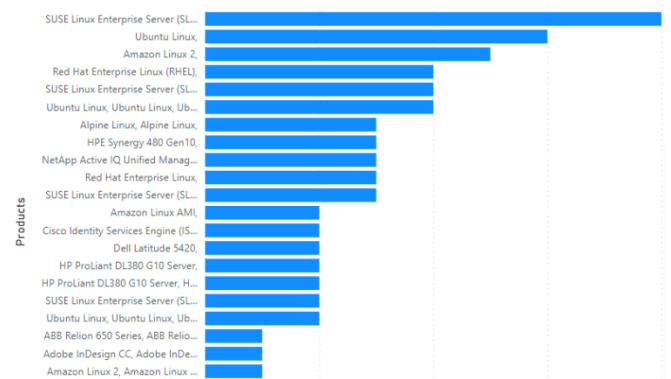
The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that present a reasonable risk to your environment.
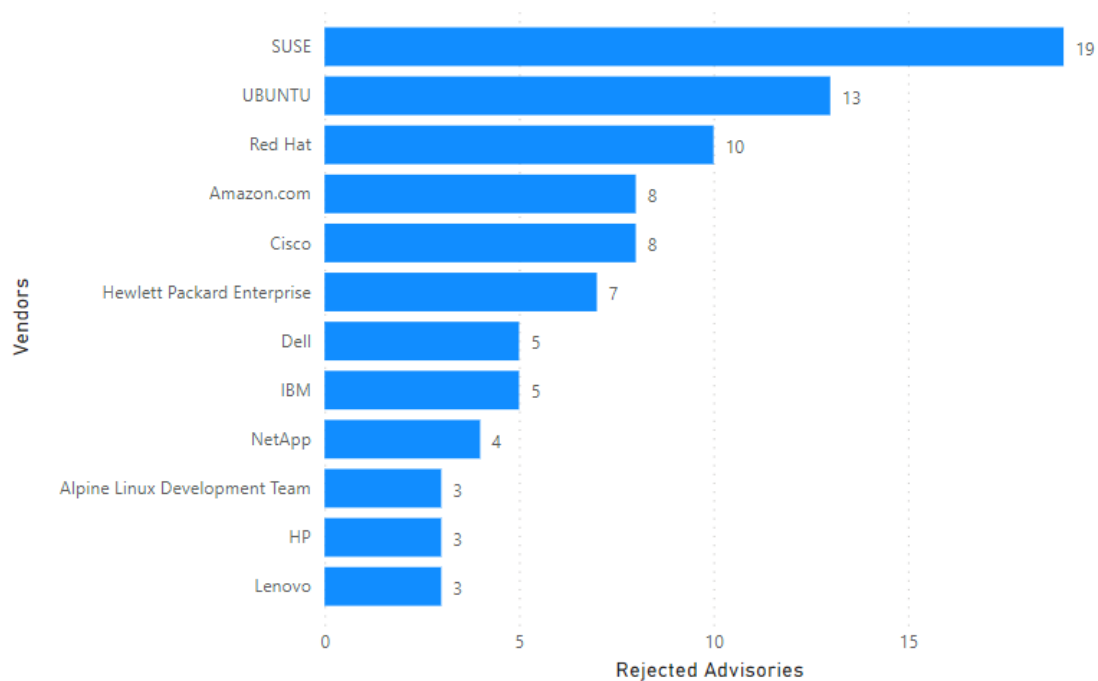
An advisory may be rejected many reasons. The most common are:

- **No reachability**

  The vulnerability cannot be exploited because the affected systems cannot be reached by an attacker.

- **No gain**

  The vulnerability may be reached, but without any gain for the attacker.

- **No exploitability**

  The vulnerability cannot be exploited because, for example, policy forbids installation of the affected software.

- **Dependent on other**

  The vulnerability cannot be exploited by itself, but depends on another vulnerability being present.

Rejected Advisories by Products

Rejected Advisories by Vendors

©2023 Flexera. All rights reserved.

All other brand and product names are trademarks, registered trademarks, or service marks of their respective owners.

8

Addressing awareness with vulnerability insights

Prevalence:
- How many systems would benefit from any given security update?
- Does it pose a risk? It's on all systems? **Patch**.

Asset Sensitivity:
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

Criticality:
- The most popular method of thoughtful prioritization.
- If exploited , how bad could it affect your security? Is it designated to be of a high criticality? **Patch**.

Threat Intelligence:
- The newest and most impactful method focuses on the likelihood of exploitation.
- Is it likely to be exploited? **Patch**.

How do we know that more insights/data is needed?

Focusing on vulnerabilities with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between 4 and 7.
Focusing
on vulnerabilities for the top 20 vendors would address only about 20 percent.

criticality	avg threat score x # of advisories
Moderately Critical	3,925.00
Highly Critical	3,082.00
Less Critical	1,418.00
Extreme Critical	437.00
Not Critical	213.00
Total	**9,075.00**

Take away 1:

Critical vulnerabilities do not necessarily present the most risk.
Leverage threat intelligence to better prioritize what demands your most urgent attention.
Organizations who do not have Threat Intelligence data should consider implementing this to ensure they have the complete picture.

Take away 2:

Most vulnerabilities have a patch available (typically within 24 hours after disclosure).
(No fix : no patch available for this insecure version, therefore need to upgrade)
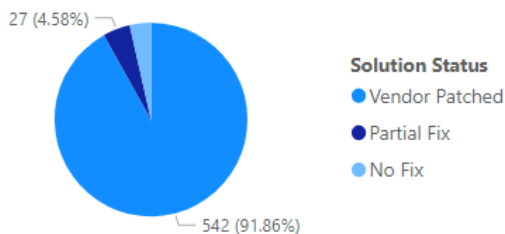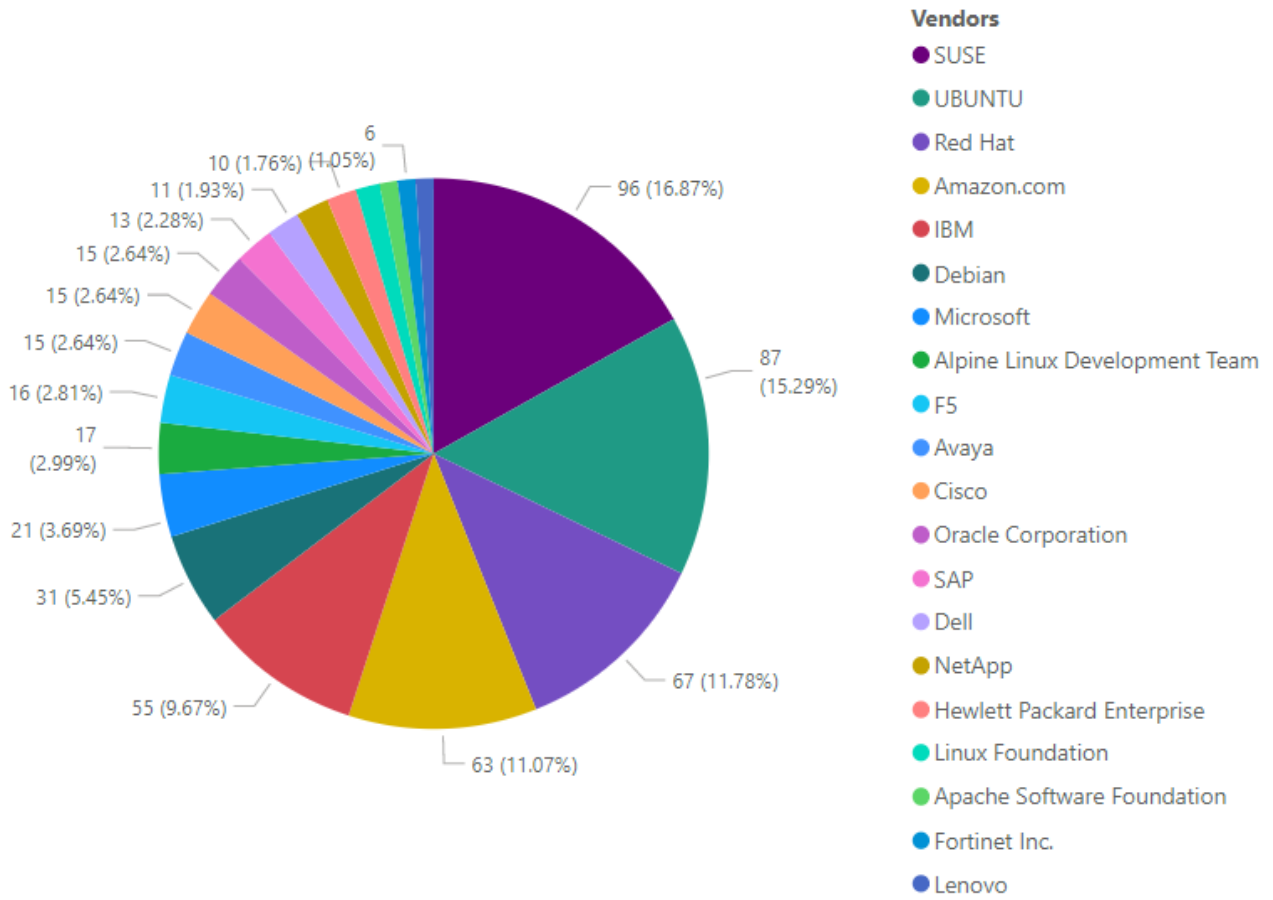

Previous month :   **480** *Vendor Patched (***76.68**%)*
This Month :   **542** Vendor Patched (**91.86%**)

* Previous monthly reports included rejected advisories which was incorrectly representing the patch status %

Vendor view

Top vendors with the most advisories

Vendors
- SUSE
- UBUNTU
- Red Hat
- Amazon.com
- IBM
- Debian
- Microsoft
- Alpine Linux Development Team
- F5
- Avaya
- Cisco
- Oracle Corporation
- SAP
- Dell
- NetApp
- Hewlett Packard Enterprise
- Linux Foundation
- Apache Software Foundation
- Fortinet Inc.
- Lenovo

Top vendors with zero-day

Pie chart:
- 1 (8.33%)
- 3 (25%)
- 8 (66.67%)

Vendors
- Microsoft
- Apple
- WebKitGTK
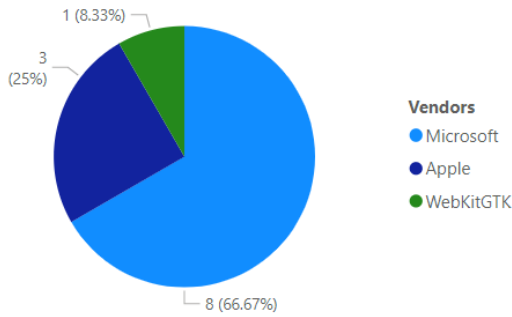
Top Vendors with highest average threat score

Bar chart — Average of cve threat score (y-axis, 0 to 80) by Vendors (x-axis):
Apple, WebKitGTK, Django Software Foundati..., Microsoft, Joyent, Inc., Michal Trojnara, Splunk, Zimbra, EMC Corporation, Sourcefire, Oracle Corporation, GitLab Inc., Kernel.org, Cent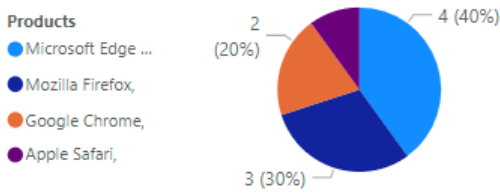OS Project, Debian, Skyhigh Security, Mozilla Foundation, Postgresql, Google, UBUNTU, Fortinet Inc., phpMyAdmin, Amazon.com, PHP Group, Python Software Foundati..., SUSE, Alpine Linux Development..., Red Hat, Samsung, NetApp, Hitachi, Huawei Device Co., Ltd., GNU Project, Citrix Systems, Adobe, Tenable, IBM, Apache Software Foundati..., HP, Linux Foundation, Avaya, SolarWinds, Cisco, Dell

Browser-related advisories

Advisories per browser

Products
- Microsoft Edge ...
- Mozilla Firefox,
- Google Chrome,
- Apple Safari,

2 (20%)
4 (40%)
3 (30%)

Browser zero-day vulnerabilities

Count of Advisories	Products	Advisories
1	Apple Safari,	SA113908
1		

Average CVSS (criticality) score per browser
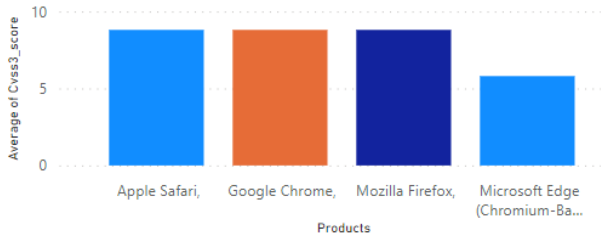
Average threat score per browser

What's the Attack Vector ?

Attack_Vector ● From Remote Network

Networking related advisories

Vendors
- F5 — 16 (29.09%)
- Cisco — 15 (27.27%)
- NetApp — 11 (20%)
- Fortinet Inc. — 6 (10.91%)
- Broadcom Corporation — 2 (3.64%)
- Arista Networks, Inc. — 1 (1.82%)
- Array Networks — 1 (1.82%)
- Huawei Device Co., Ltd. — 1 (1.82%)
- McAfee — 1 (1.82%)
- Palo Alto Networks — 1
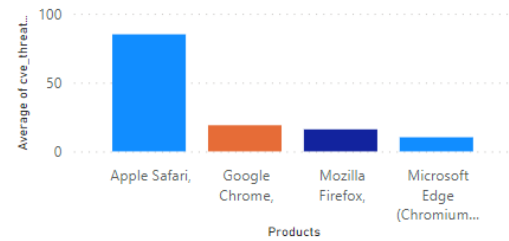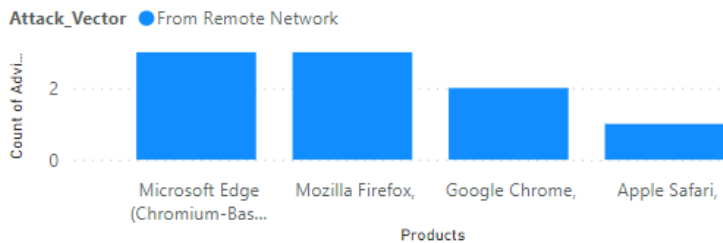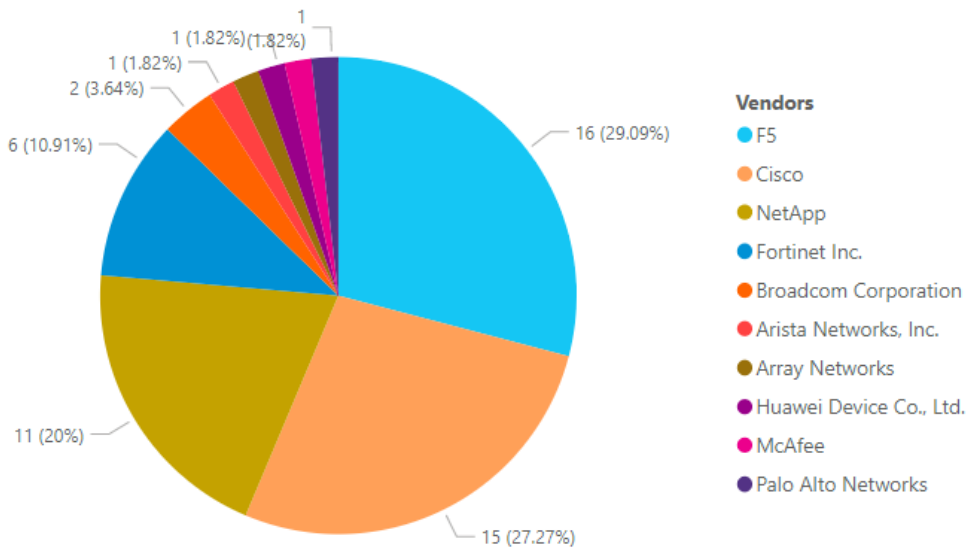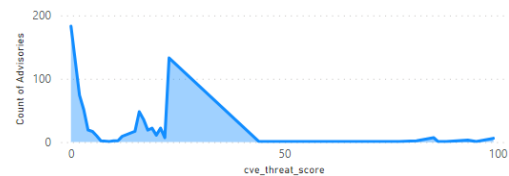
Threat intelligence

In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually being exploited in the wild.

Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, Threat Intelligence augments Software Vulnerability Research's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

Count of malware-exploited CVEs
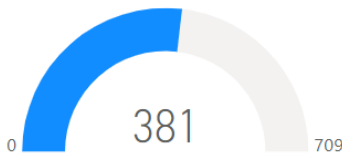
Count of advisories by CVE threat score

Threat intelligence advisory statistics:

SAIDs with a threat score (1+)	**526↑(**416*)*	74.19%
SAIDs with no threat score (=0)	**183↑(***210)*	25.81%

SAID: Secunia Advisory Identifier

Range	# SAIDS	Last month
Medium-range threat score SAIDs (13-23)	**315 ↑**	**(263)**
Low-range threat score SAIDs (1-12)	**187 ↑**	**(113)**
Very critical threat score SAIDs (71-99)	22 ↑	(16)
High-range threat score SAIDs (24-44)	1 ↓	(13)
Critical-range threat score SAIDs (45-70)	1 ↓	(11)

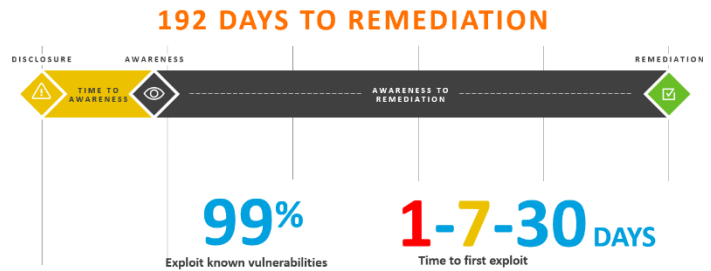More information about how the Secunia team calculates the threat score :

- Evidence of exploitation
- Criteria for the threat Score Calculation
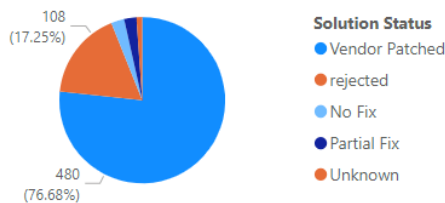- Threat Score Calculation - Examples

Patching

Most of this month's vulnerabilities are vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.

The challenge remains that organizations do not have full visibility or awareness when a vulnerability is disclosed (time to awareness). Another big challenge is the time to remediation (the time from having this information, correlating that with your environment and initiating the process to get the software updated to a secure version).

The Risk Window

192 DAYS TO REMEDIATION

DISCLOSURE | AWARENESS | AWARENESS TO REMEDIATION | REMEDIATION
TIME TO AWARENESS

99%
Exploit known vulnerabilities

1-7-30 DAYS
Time to first exploit

Vulnerabilities that are vendor patched

Solution Status
- Vendor Patched
- rejected
- No Fix
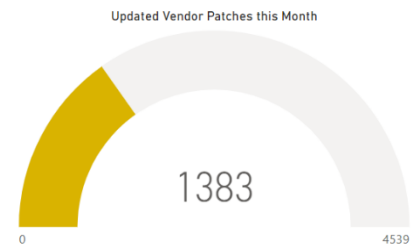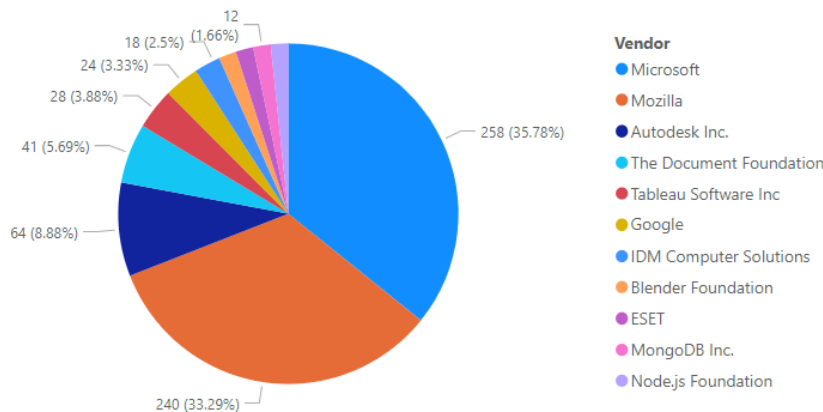- Partial Fix
- Unknown

108 (17.25%)
480 (76.68%)

Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(More than 4,500)** in the world. This helps customers act quicker and save time by offering an integrated approach to effectively locate, prioritize threats and remediate them quickly to lower the risk to your organization.

This month's top vendor patches

(Updated Patches per vendor)

Updated Vendor Patches this Month

1383
0   4539

12 (1.66%)
18 (2.5%)
24 (3.33%)
28 (3.88%)
41 (5.69%)
64 (8.88%)
258 (35.78%)
240 (33.29%)

Vendor
- Microsoft
- Mozilla
- Autodesk Inc.
- The Document Foundation
- Tableau Software Inc
- Google
- IDM Computer Solutions
- Blender Foundation
- ESET
- MongoDB Inc.
- Node.js Foundation

More information

Below a few links with information about how Flexera can help you with creating an effective software vulnerability and patch management process to reduce security risk.

- Flexera's Software Vulnerability Manager landing page

- Request a trial / demo

- Flexera's Community Pages with lots of great resources of information including:

  o Software Vulnerability Management Blog

  o Software Vulnerability Management Knowledge Base

  o Product Documentation

  o Forum

  o Learning Center

About Flexera

Flexera delivers SaaS-based IT management solutions that enable enterprises to accelerate digital transformation and multiply the value of their technology investments. We help organizations inform their IT with unparalleled visibility into complex hybrid ecosystems. And we help them transform their IT with tools that deliver the actionable intelligence to effectively manage, govern and optimize their hybrid IT estate.

More than 50,000 customers subscribe to our technology value optimization solutions, delivered by 1,300+ passionate team members worldwide. To learn more, visit flexera.com