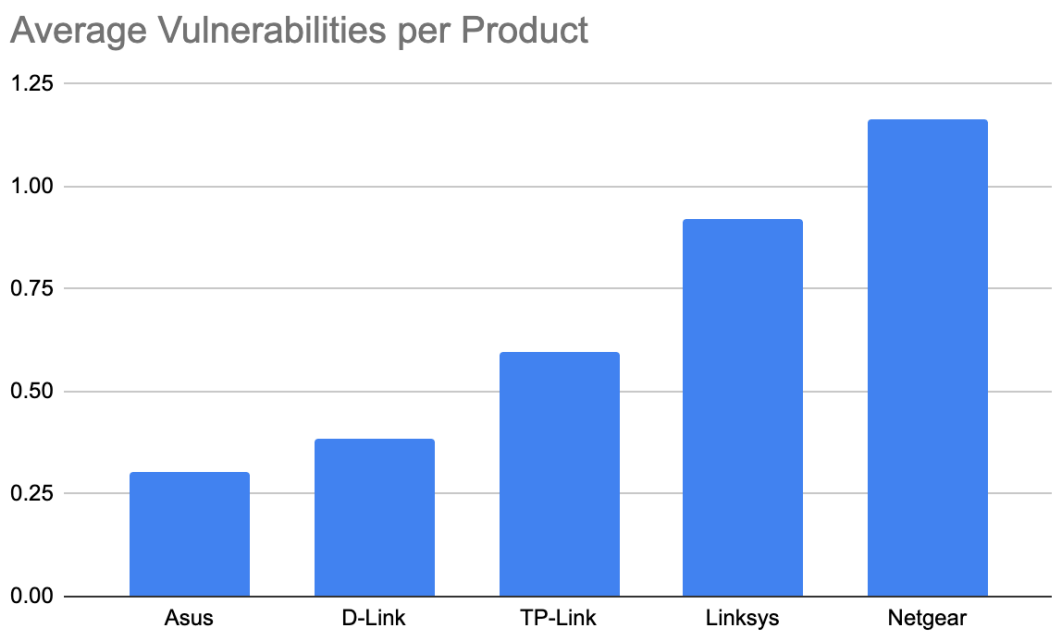
TP-Link Vulnerabilities vs. Industry

I. Data from CVE Details

Much of our data comes from https://www.cvedetails.com/.

You can look up this data for each of these companies (and others) individually.

Here is a basic graph that shows an average number of vulnerabilities per product for each of these wireless router OEMs (note: this shows raw - not weighted - vulnerability numbers for the past 12 years).



The details of known vulnerabilities (CVEs) for several different vendors can be found below:

- TP-Link: https://www.cvedetails.com/vendor/11936/
- Netgear: https://www.cvedetails.com/vendor/834/
- D-Link: https://www.cvedetails.com/vendor/899/
- Linksys: https://www.cvedetails.com/vendor/833/
- Asus (makes other stuff, too): https://www.cvedetails.com/vendor/3447/

The summary results (reflected in the bar graph above) for the past 12 years are:

- TP-Link: 648 products, 388 vulnerabilities
- Netgear: 1042 products, 1213 vulnerabilities
- D-Link: 486 products, 186 vulnerabilities
- Linksys: 111 products, 102 vulnerabilities
- Asus: 929 products, 281 vulnerabilities

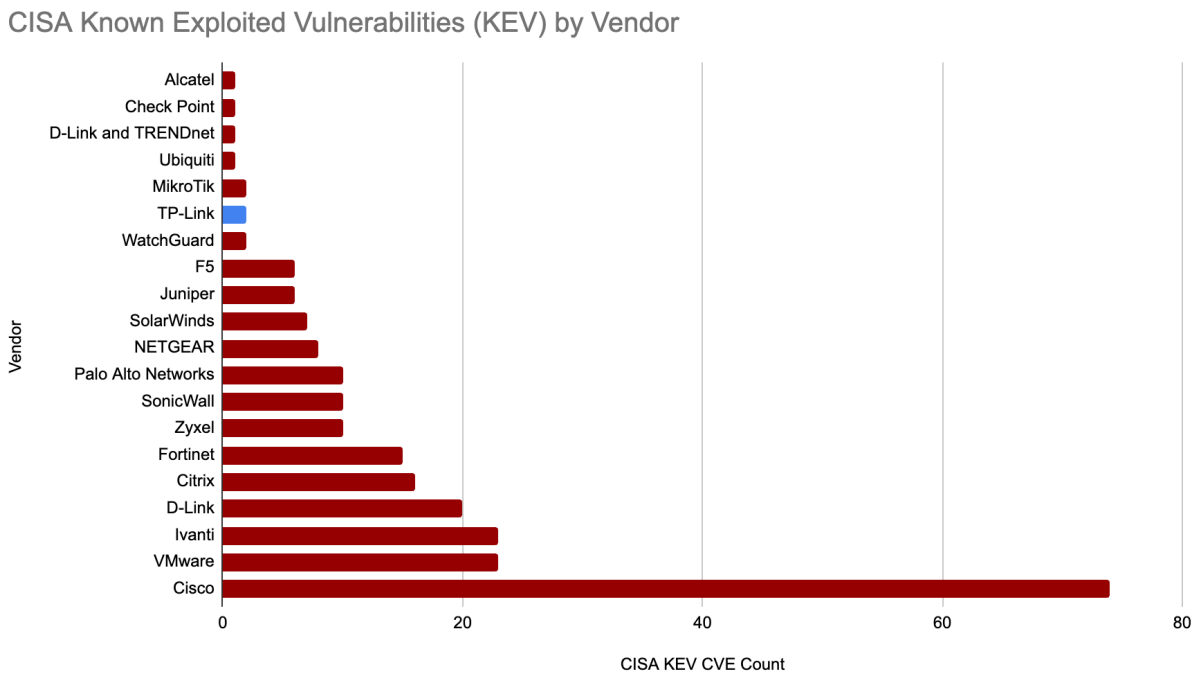
Note: When you do a lookup on individual companies, it will show you the weighted CVSS score (which accounts for the severity level of each vulnerability) *only for the past year*. Here's what those scores look like for the last year and for the last 10 years:

Manufacturer	Weighted CVSS Score for the past 12 months	Weighted CVSS score for the past 10 years
TP-Link	7.7	8.6
Netgear	7.8	8.1
D-Link	8.3	8.6
Linksys	8	8.6
Asus	6.9	7.8

II. CISA KEV Data

There is also ample data available from CISA's Known Exploited Vulnerabilities (KEV) catalog. These are vulnerabilities that are known to have been actively exploited by threat actors, and thus, they are the most serious. You can download the entire database and create pivot tables/graphs.

We've created this one. (You can validate it by looking up each company individually.)



Here is the same data in a different format:

Vendor	Count of Known Exploited Vulnerabilities
Alcatel	1
Check Point	1
D-Link and TRENDnet	1
Ubiquiti	1
MikroTik	2
TP-Link	**2**
WatchGuard	2
F5	6
Juniper	6
SolarWinds	7
NETGEAR	8
Palo Alto Networks	10
SonicWall	10
Zyxel	10
Fortinet	15
Citrix	16
D-Link	20
Ivanti	23
VMware	23
Cisco	74

III. Vulnerabilities Exploited by Chinese Threat Actors

TP-Link is not uniquely targeted, supported by the following facts:

- Not a Single-Vendor Issue:
  The recent campaigns by Chinese state-sponsored groups like Volt Typhoon and Salt Typhoon have affected network equipment across the industry. TP-Link, ASUS, Cisco, D-Link, Netgear, Zyxel, Fortinet, and Sophos have all been cited in threat intelligence reporting. This clearly demonstrates that these actors are not singling out TP-Link devices.
- Broad Exploitation Strategy:
  These threat actors systematically look for any exploitable vulnerabilities—outdated firmware, known software flaws, or misconfigurations—regardless of the manufacturer. Their tactics are

opportunistic, targeting any widely deployed brand to gain unauthorized access and maintain persistence.

- Industry-Wide Challenge:
  Because these campaigns span multiple leading vendors, the issue reflects an industry-wide challenge rather than a specific vendor shortcoming. TP-Link's experience is consistent with what many reputable companies face in the evolving cybersecurity landscape.
- Critical Importance of Patching and Configuration:
  Like many vendors, TP-Link emphasizes regular firmware updates, timely patching, and proper security configurations. The fact that multiple brands are impacted underscores the universal importance of following best practices to secure devices.
- Industry and Government Collaboration:
  TP-Link's ongoing commitment to security, alongside participation in government-led initiatives and adherence to evolving standards (like the EU Cyber Resilience Act and the U.S. Cyber Trust Mark), shows that we are working to strengthen defenses industry-wide. The shared nature of the threat environment encourages closer collaboration among vendors, regulators, and consumers.
- Conclusion:
  The presence of Volt Typhoon and Salt Typhoon across various reputable brands confirms that these threat actors do not target TP-Link uniquely. Instead, they exploit any available vulnerabilities, underscoring the need for collective, proactive measures to reinforce security across the entire ecosystem.

Sources for above:

- https://www.tenable.com/blog/volt-typhoon-u-s-critical-infrastructure-targeted-by-state-sponsored-actors
- https://www.csoonline.com/article/3604173/volt-typhoon-returns-with-fresh-botnet-attacks-on-critical-us-infrastructure.html
- https://www.wired.com/story/sophos-chengdu-china-five-year-hacker-war

IV. Source Data from CVE Details

Here is a chart from CVE Details showing data over time for TP-Link.

Tp-link : Vulnerability Statistics

Products (648) Vulnerabilities (388) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	3	1	0	1	0	0	0	0
2015	0	0	0	0	1	0	1	0	0	0	0
2016	0	0	0	0	0	0	0	0	0	0	0
2017	1	0	0	2	1	0	0	0	0	0	2
2018	4	2	0	4	1	0	3	0	0	0	6
2019	5	4	0	2	1	0	1	0	0	0	1
2020	6	2	0	2	1	0	1	0	0	0	1
2021	3	0	0	2	0	0	1	0	0	0	0
2022	19	7	0	1	0	0	0	0	0	0	1
2023	13	6	0	0	0	0	0	0	0	0	0
2024	12	2	0	1	0	0	0	0	0	0	0
Total	63	23		17	6		8				11

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	2	0
2015	0	0	0	0	0
2016	0	0	0	0	0
2017	2	2	2	1	0
2018	3	1	1	7	2
2019	4	0	0	4	0
2020	12	4	3	4	0
2021	6	0	0	3	0
2022	31	0	0	14	0
2023	6	4	3	14	0
2024	15	0	0	4	2
Total	79	11	9	53	4

TP-Link: https://www.cvedetails.com/vendor/11936/

The same chart for Netgear:

Netgear : Vulnerability Statistics

Products (1042) Vulnerabilities (1213) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	1	0	0	1	0	0	0	0	0	0	0
2015	0	0	0	0	0	0	0	0	0	0	0
2016	2	0	0	0	1	0	0	0	0	0	2
2017	2	0	0	0	1	0	1	0	0	0	1
2018	0	0	0	0	0	0	0	0	0	0	0
2019	1	3	1	3	2	0	3	0	0	0	0
2020	151	105	1	133	1	0	27	0	0	0	13
2021	37	20	0	24	4	0	2	0	0	0	0
2022	19	20	1	1	0	0	0	0	0	0	1
2023	17	3	0	17	0	0	1	0	0	0	0
2024	9	1	7	1	2	0	0	0	0	0	0
Total	239	152	10	180	11		34				17

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	1	0	0	1	0
2015	0	0	0	0	0
2016	1	1	1	6	2
2017	4	0	0	0	4
2018	0	0	0	0	2
2019	1	2	2	3	3
2020	20	22	29	20	21
2021	18	7	10	12	11
2022	7	2	2	5	0
2023	13	2	2	3	0
2024	31	0	5	14	6
Total	96	36	51	64	49

Netgear: https://www.cvedetails.com/vendor/834/

The same chart for D-Link:

D-link : Vulnerability Statistics

Products (486) Vulnerabilities (186) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	1	2	0	1	0	0	0	0
2015	0	0	0	2	0	0	0	0	0	0	0
2016	1	0	0	0	0	0	0	0	0	0	0
2017	1	0	0	2	2	0	4	0	0	0	3
2018	12	9	0	4	0	0	0	0	0	0	0
2019	1	1	0	1	0	0	1	0	0	0	1
2020	2	1	0	1	0	0	0	0	0	0	0
2021	0	0	0	0	0	1	0	0	0	0	0
2022	0	0	0	0	0	0	0	0	0	0	0
2023	1	0	0	0	0	0	0	0	0	0	0
2024	24	1	0	0	0	0	0	0	0	0	0
Total	42	12		11	4	1	6				4

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	0	0
2015	0	0	0	0	0
2016	1	0	0	0	0
2017	2	4	4	2	3
2018	16	3	2	2	1
2019	0	1	1	0	1
2020	1	0	0	0	1
2021	2	0	0	0	0
2022	0	0	0	0	0
2023	13	1	1	0	0
2024	16	0	0	2	2
Total	51	9	8	6	8

D-Link: https://www.cvedetails.com/vendor/899/

The same chart for Linksys:

Linksys : Vulnerability Statistics

Products (111) Vulnerabilities (102) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	1	0	0	0	0	0	1	0
2017	0	0	0	0	0	0	1	0	0	0	0
2018	0	0	0	0	0	0	1	0	0	0	0
2019	0	0	0	0	1	0	0	0	0	0	0
2020	0	1	0	1	0	0	0	0	0	0	0
2022	1	1	0	0	0	0	0	0	0	0	0
2023	1	2	0	0	0	0	0	0	0	0	0
2024	2	0	0	0	0	0	0	0	0	0	0
Total	4	4		2	1		2			1	

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	0	1
2017	1	0	0	0	0
2018	0	0	0	0	0
2019	0	1	1	0	0
2020	0	0	0	1	0
2022	0	0	0	0	1
2023	0	0	0	0	0
2024	1	0	0	1	3
Total	2	1	1	2	5

Linksys: https://www.cvedetails.com/vendor/833/

The same chart for Asus:

Asus : Vulnerability Statistics

Products (929) Vulnerabilities (281) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	1	0	0	1	0	0	0	0	0	0	0
2015	1	0	0	3	0	0	2	0	0	0	1
2017	4	0	0	2	0	0	2	0	0	0	0
2018	2	2	0	6	0	0	3	1	0	0	1
2019	4	1	0	1	1	0	1	0	0	0	2
2020	0	1	0	2	0	1	1	0	0	0	1
2021	32	1	0	1	5	0	0	0	0	1	0
2022	6	6	2	4	3	0	0	0	0	0	3
2023	8	0	1	3	1	0	0	0	0	0	0
2024	3	0	1	3	0	0	0	0	0	0	0
Total	61	11	4	26	10	1	9	1		1	8

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	2	1	1	0	1
2015	1	0	0	1	1
2017	4	1	2	1	3
2018	1	2	2	4	2
2019	1	0	1	6	0
2020	0	0	0	2	4
2021	1	2	2	3	0
2022	2	0	2	4	0
2023	5	1	1	4	1
2024	2	0	0	1	1
Total	19	7	11	26	13

Asus (makes other stuff too): https://www.cvedetails.com/vendor/3447/