Germany, Switzerland and the Netherlands are the fastest to secure their vulnerable Citrix systems

Since 11.01.2020, Alpha Strike Labs of Limes Security GmbH has been performing scans for vulnerable Citrix systems with the vulnerability CVE-2019-19781, which according to current media reports and Twitter comments is already being actively exploited. For scan acquisition, they use the DCS scan network with over 1000 different search nodes [1], which was presented at CCCamp 2019.

A chronological analysis shows that Germany, Switzerland and the Netherlands patched about 85-90% of the Citrix servers that were originally vulnerable on January 21, 2020. Other countries such as China, France and the USA, on the other hand, only achieve a patch rate of 24-56%. On 11.01. there were 49,492 vulnerable Cirtix servers worldwide and on 21.01. there were still 18,620 vulnerable systems.

In Germany, about 24 hours after the Citrix patch was made available, "only" about 800 and in Austria 137 Citrix servers freely accessible from the Internet were affected by the vulnerability. While 171 clinics and hospitals were still affected at the first scan time in Germany, Austria and Switzerland (DACH region) on 11.01.2020. About 5 days later there were only 31 Citrix instances and another 5 days later only 6 vulnerable systems. However, more than 140 energy suppliers such as public utilities were also affected at the first scan time. At the current point in time (21.01.2020), there are still 21 utilities that have a vulnerable Citrix service.

The public sector, which includes above all the state and federal authorities, also poses a major problem. Here 212 servers were affected on 11.01. and currently only 21 servers were affected. If one takes into account that the first scan was carried out about 3 weeks after the vulnerability became known in mid-December, this shows that the public administration in the DACH region also has some catching up to do in the area of patch or security management.

It is a good sign that many systems no longer have this vulnerability, but it is also frightening how long it takes to apply the patch or hotfix to the operators of these systems worldwide.

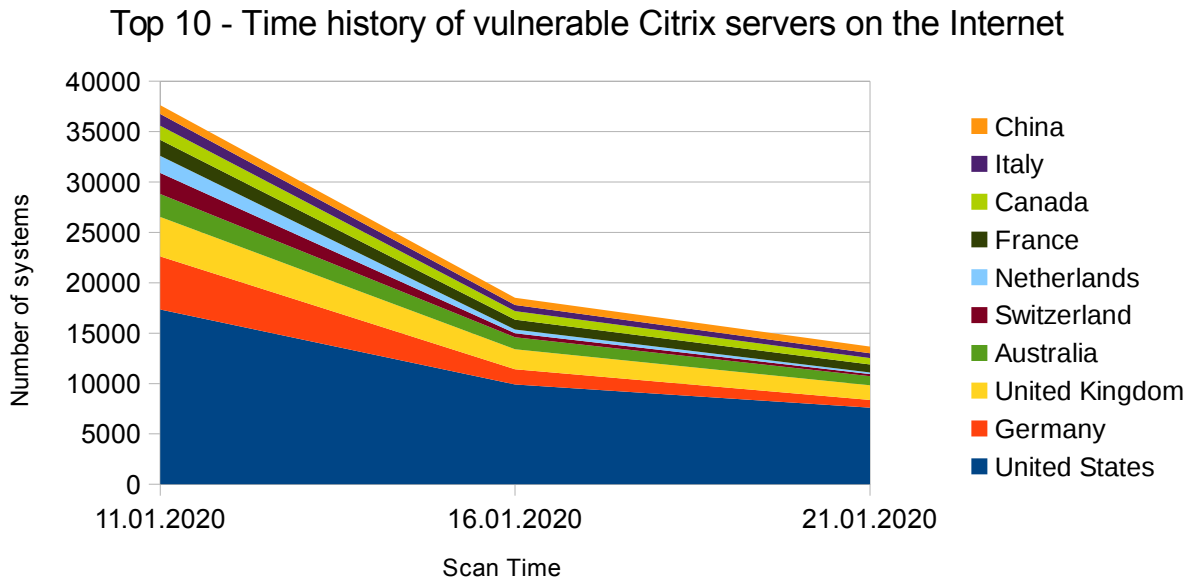


Figure 1

Land	11.01.2020	16.01.2020	21.01.2020	Absolute difference	Relative Difference (1=100%)
Switzerland	2113	408	202	-1911	-0,90
Netherlands	1689	365	170	-1519	-0,90
Germany	5265	1515	784	-4481	-0,85
United Kingdom	3920	1985	1459	-2461	-0,63
Australia	2273	1177	889	-1384	-0,61
Italy	1172	600	479	-693	-0,59
United States	17341	9911	7601	-9740	-0,56
Canada	1399	853	633	-766	-0,55
France	1594	981	781	-813	-0,51
China	870	702	660	-210	-0,24

Table 1: Top 10 - Time history of vulnerable Citrix servers on the Internet

	Banking	Education	Hospitals	Government	Energy Provider
2020-01-11	44	108	171	212	141
2020-01-16	7	8	31	61	48
2020-01-21	5	6	6	21	21

Table 2: Number of vulnerable Citrix servers by category and scan time Region: Germany, Austria, Switzerland

A Geo-IP resolution of the vulnerable servers shows the distribution of the systems in Europe over time.

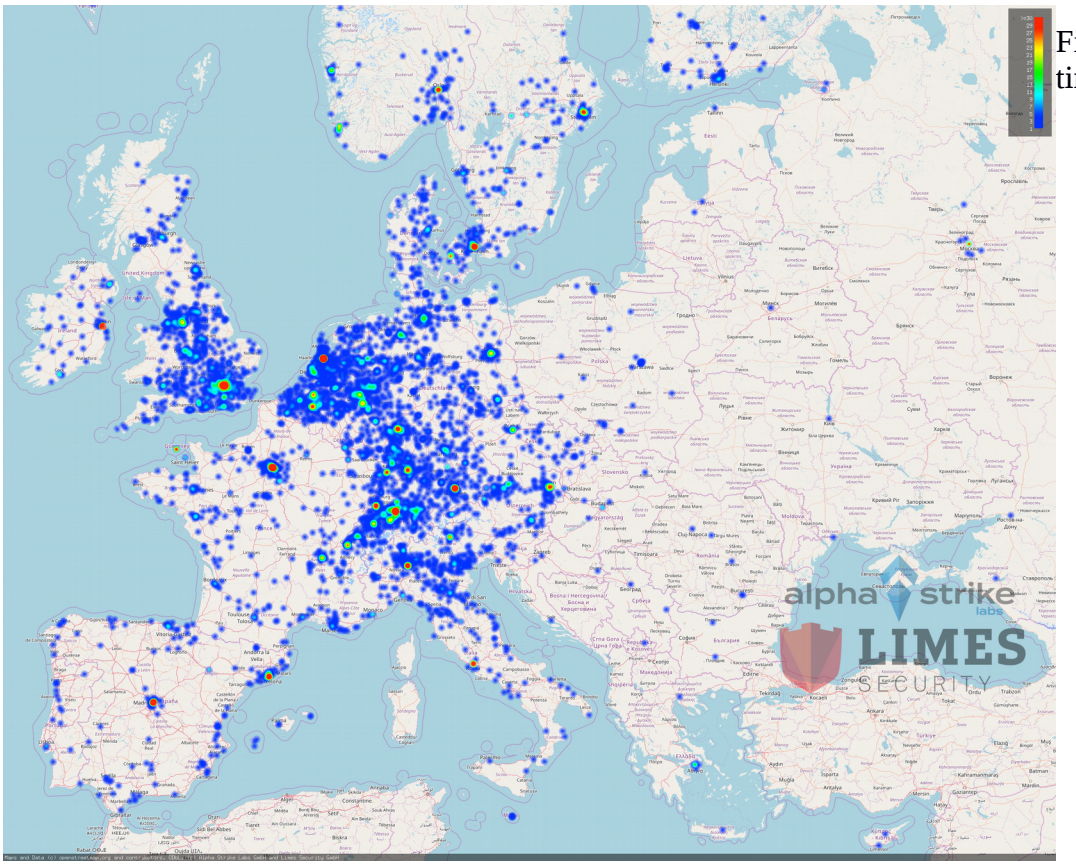


Figure 2: Scan time 2020-01-11

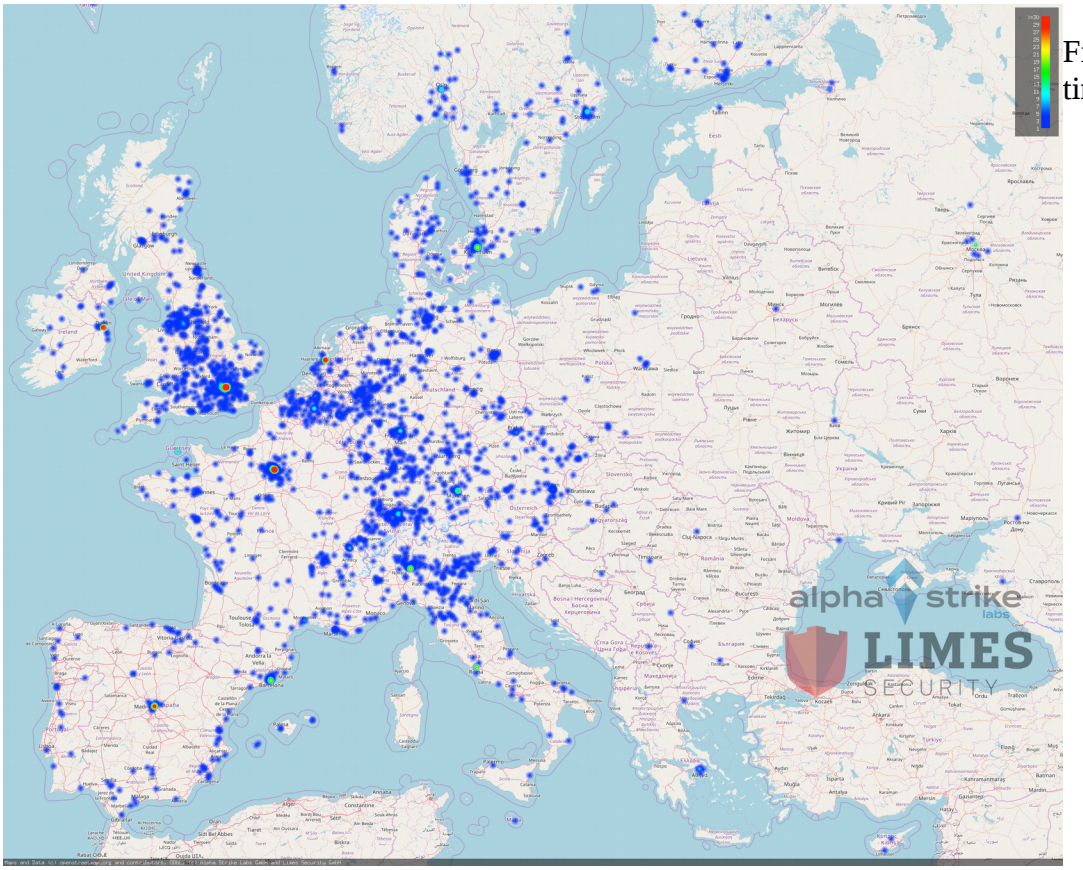
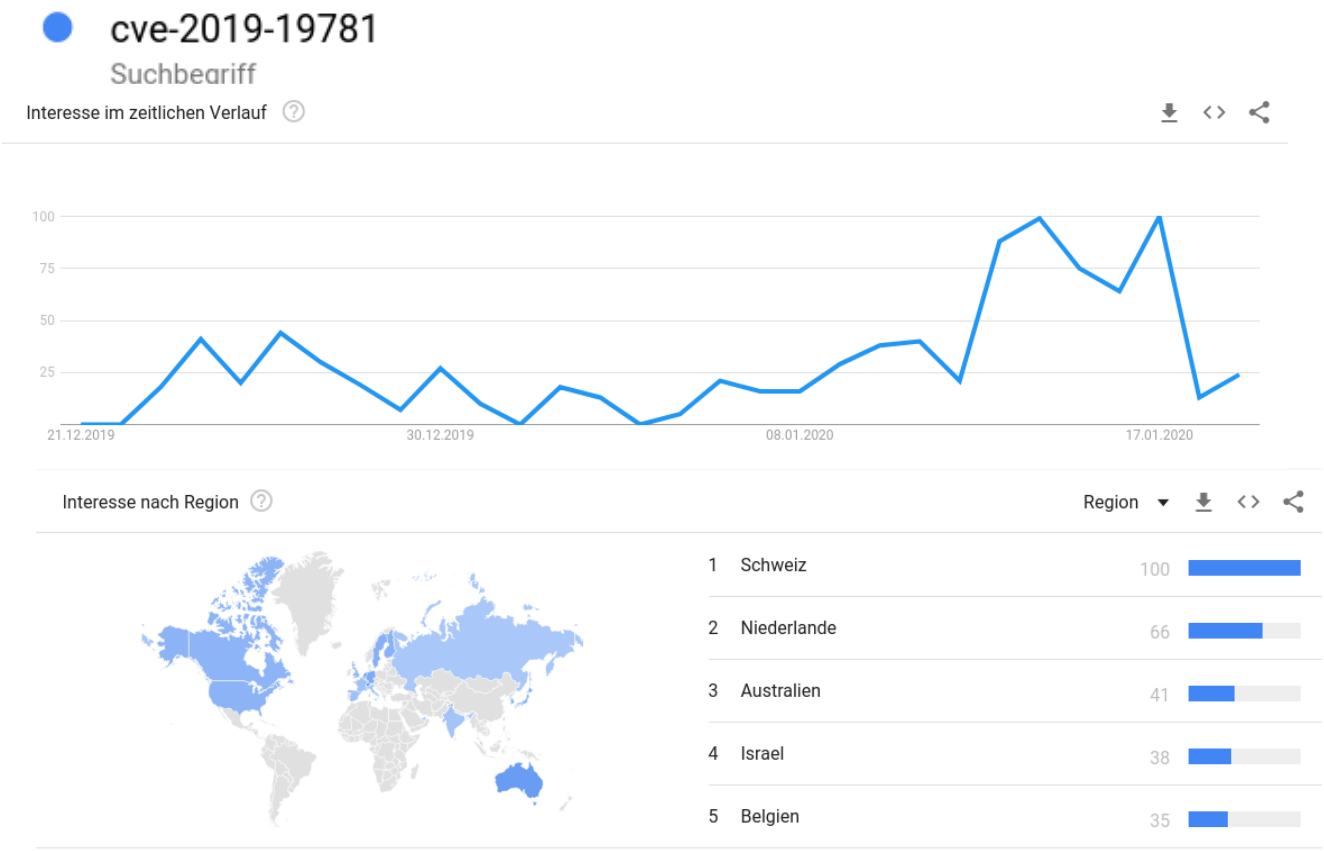


Figure 3: Scan time 2020-01-21

However, the analyses show large differences between countries in terms of patch time. It is very difficult to investigate the causes of this. However, if you look at the countries with Google search queries for the Citrix vulnerability with CVE number "cve-2019-19781", you can immediately see that the countries with the highest patch level of 90%, Switzerland and the Netherlands, are also the countries with the most search queries for this vulnerability.
Furthermore, it can quickly be seen that from 13.01.2020 onwards, the interest of Google users in the vulnerability has increased significantly. At the same time, the scan data shows that after 13.01.20, the protection of the systems has also increased considerably. This is certainly also connected with the increased media coverage.

Since 2012, **Limes Security GmbH** has been offering manufacturer-independent security consulting in the areas of OT Security and secure software development. Her clients are mainly well-known national and international companies from the production and critical infrastructure sector. Limes Security was also recently awarded the "Club of Winners" for its sustainable corporate management in the Best Business Awards.

Alpha Strike Labs is the development and research team of Limes Security GmbH. Topics range from the simulation of real hacker attacks, the detection of potential external attack sites using open source intelligence and global comprehensive Internet scans to the creation of individual IoT security concepts. The innovative approaches of Alpha Strike Labs were also honoured at the UP18@it-sa Security Start-Up Competition with a nomination among the best 18 Security Start-Ups 2018 in the DACH region.



Picture source: [2]

[1] https://media.ccc.de/v/Camp2019-10353-fast_global_internet_scanning_-_challenges_and_new_approaches#t=3

2] Interest over time in Google Trends for cve-2019-19781 - Worldwide, View last 30 days - https://trends.google.com/trends/explore/TIMESERIES/1579634400?hl=dez=-60ate=today+1-m&q=cve-2019-19781&sni=3

Contact:

Johannes Click
CEO

[e-mail] j.klick@alphastrike.io
[Fax] You think I have fax?
[phone] +49 (0) 30 1208 77420
[Mobile] +49 (0)176 444 30475

Alpha Strike Labs GmbH
Albert-Einstein-Str. 14
12489 Berlin
Germany

CEO: Johannes Klick, Tobias Zillner
Commercial Register: AG Berlin-Charlottenburg, HRB 190512

====

Peter Panholzer
Managing Director/General Manager

Phone: +43 664 163 1139

Email: ppa@limessecurity.com
Web: www.limessecurity.com

Limes Security GmbH
Software Park 26
4232 Hagenberg
Austria

FN: 390566 m; FB court: Linz;
Information Technology and
Software development