Second Empirical Study on the Cyber Security of Lebanon - 653 Low Hanging Critical Vulnerabilities

Saturday, 02 January, 2021 by Lebanon CERT

Summary of Findings

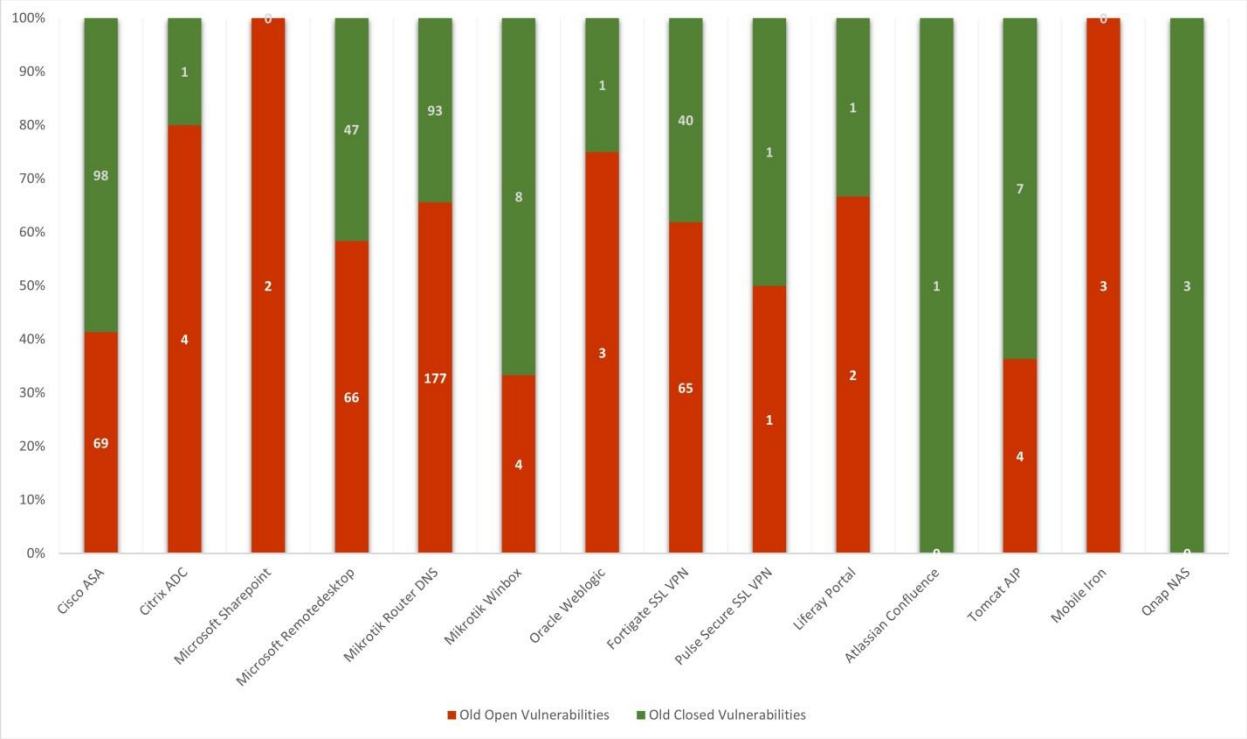
A study conducted by researchers from Lebanon Cybersecurity Empowering Research Team (Lebanon CERT) in the fourth quarter in 2020 revealed 653 critical security vulnerabilities in a sample of 39 620 information systems from various Lebanese sectors (banking, technology, insurance, education, governmental and others). This study, a second of its kind, was focused on evaluating information systems in Lebanon in various sectors, by examining the exposure of these systems to hacking through some of the recently published software vulnerabilities. 39 620 information systems and 13 software products with known critical vulnerabilities were selected. The security of these systems against the selected vulnerabilities was tested. The results showed 653 vulnerable information systems that can be easily hacked by a novice hacker to have full control over these systems.

Example Impact of the Selected Critical Vulnerabilities:

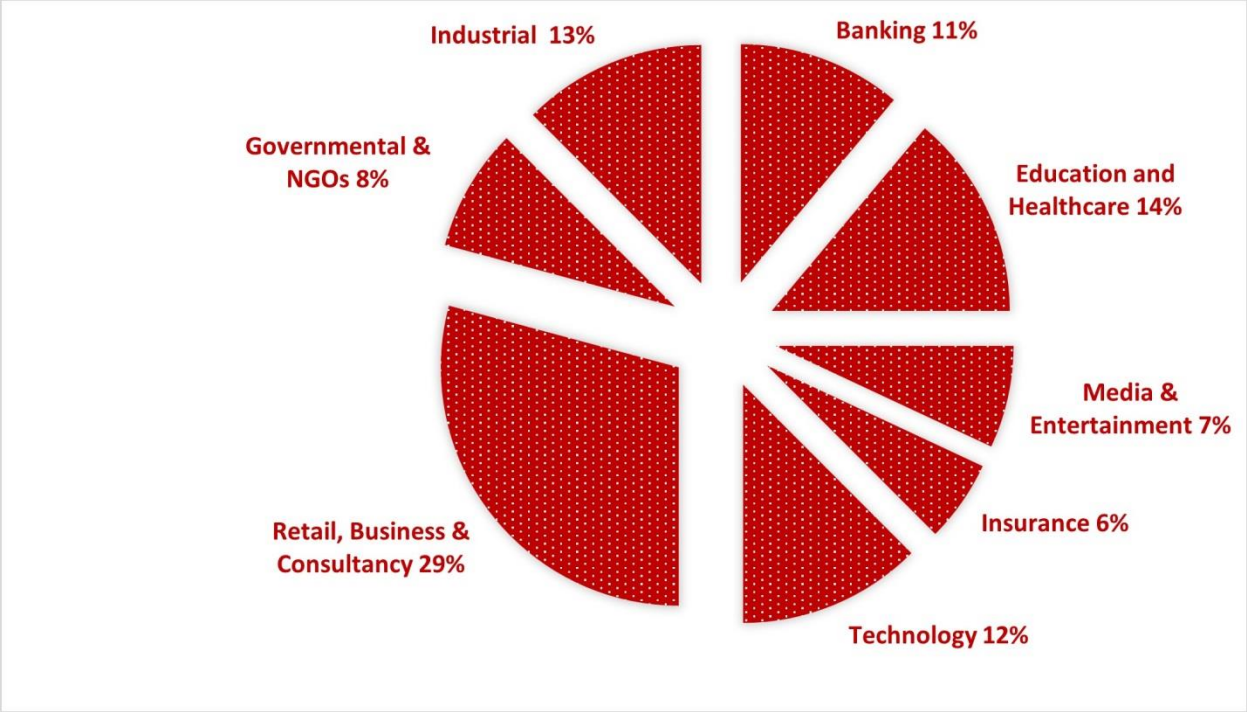
It is worth to mention that some of the security vulnerabilities that were examined during this study were exploited by hackers to attack a number of international companies such as the United Nations, Essilor Luxottica, Dusseldorf University Hospital and others [1,2,3].

Our Evaluation of the Attack Surface of Lebanon

This study comes after a first study published in an international scientific conference and was covered by Al-Akhbar newspaper in a special report published on 12 Sep. 2020 and other Lebanese media [4]. The first study [5] identified 1645 critical security vulnerabilities in 24 382 information systems that were analyzed. Apart from uncovering critical vulnerabilities, the study also addressed the responsiveness of the information systems administrators; indeed, multiple emails were sent - during the first study – to the administrators of the identified vulnerable information systems, to explain the vulnerabilities and the necessary patches. During the second study, these systems were scanned several times again for the same previously identified vulnerabilities. It was found that 57% of the systems (400 still exposed systems in the fourth quarter of 2020 out of 701 in the third quarter) have not been patched yet. A detailed overview of these findings is depicted below.



Apart from that, 253 newly exposed vulnerabilities were discovered (using one of the 13 selected vulnerabilities). To recap, the selected vulnerabilities are i) considered severe and remotely exploitable, ii) have a Proof-of-Concept (PoC) exploit available online, and iii) can cause serious damage to critical sectors in the country, if affected. As such and using a sample of 71 vulnerable systems, we have analyzed the distribution of these vulnerabilities among the Lebanese sectors. Unfortunately, our analysis shows (see below) that the vulnerabilities are affecting the majority of the Lebanese sectors, including critical infrastructure including banking!



Our Core Message

The work conducted and the results obtained revealed the lack of applying two core best practices in information security which are:

1. patch management
2. incident handling

The lack of awareness with respect to information security risks, even for some administrators of information systems, is also noteworthy.

Our Response: Launching Lebanon CERT

Hence the importance of the initiative taken by the researchers to establish the Lebanon Cybersecurity Empowering Research Team (Lebanon CERT). It is a group of Lebanese cybersecurity experts who seek to empower the cyber space in Lebanon and to spread and raise security awareness within the community against the threats that face the digital systems of the different Lebanese sectors.
Lebanon CERT team aims to provide a more secure digital space for public and private sectors including banking, telcos, educational institutes, entertainment, business, and many others. To this end, Lebanon CERT yields a continuous assessment of the attack surface in the Lebanese perimeter in order to capture critical vulnerabilities through which an unskilled or skilled hacker is capable of fully compromising the existing information systems. Once captured, the vulnerabilities will be reported in time to the corresponding actor via a detailed email that

includes all necessary steps to avoid any possible cyber-attack to the exposed system.
In addition, the team works to inform any institution whose system is identified to have a critical vulnerability by sending an e-mail containing all the details that help in avoiding any possible cyber-attack. It also aims to raise awareness about cyber security risks and their repercussions on all sectors, and to help these sectors to continuously protect their digital systems.
The researchers are always looking to enhancing cyber security level in Lebanon by involving international cyber security firms, Lebanese ISPs, system administrators, research teams, and delegated staff from the public sector in the evaluation and remediation of Lebanon's attack surface.

References

[1] Zeljka Zorz, Jan. 2020, https://www.helpnetsecurity.com/un-hacked
[2] Pierluigi Paganini, Sept. 2020, https://securityaffairs.co/luxottica-hacked
[3] William Ralston, Nov. 2020, https://www.wired.co.uk/hospital-death-germany
[4] Ali Awad, Sep. 2020, https://al-akhbar.com/Community/critical-vulns
[5] Lebanon CERT, Jun. 2020, https://lebanoncert.org/study-q1-2020