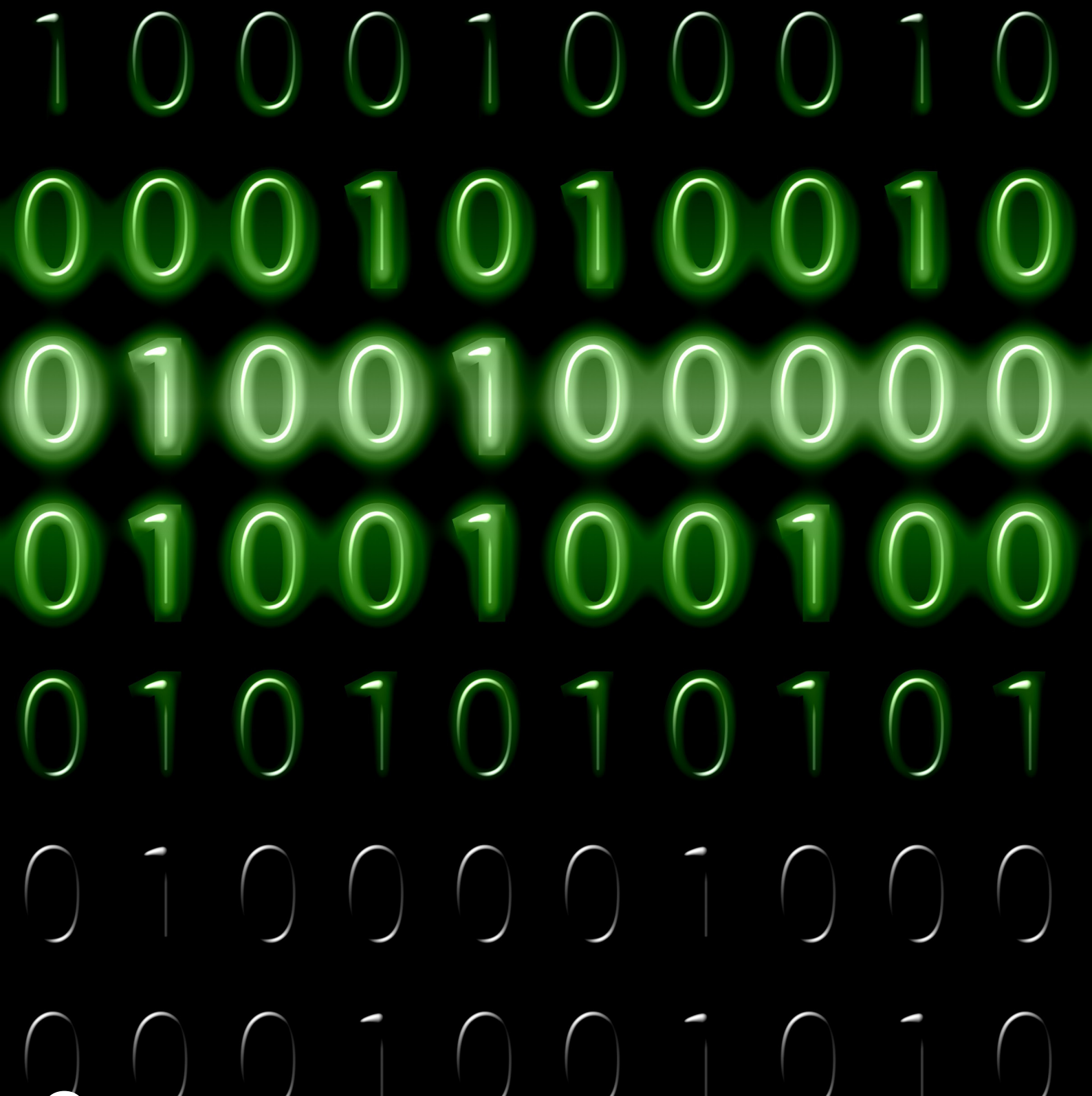
Cyberwatch Finland

WEEKLY REVIEW

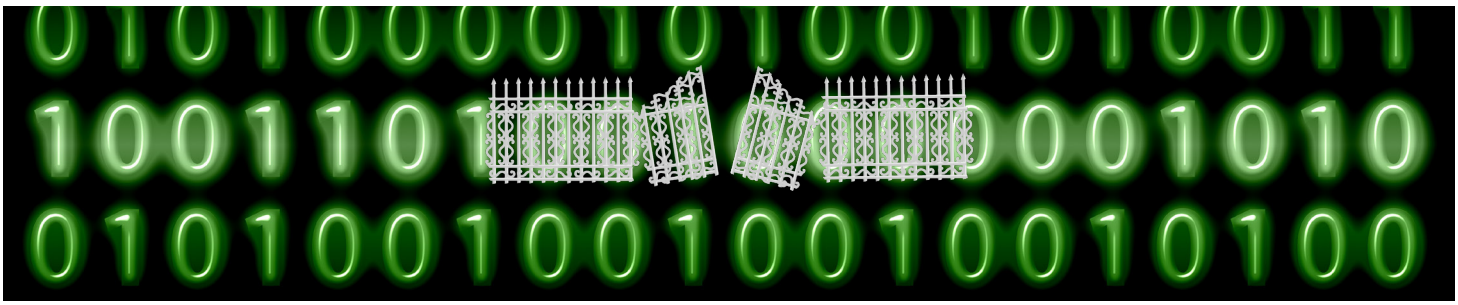
15/2024



Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

15/2024



WHO IS RESPONSIBLE FOR OPEN SOURCE SECURITY

At the beginning of April, the news threshold was crossed by an incident that a backdoor had been deliberately infiltrated into an open-source code library. One of the developers of the code was involved in the event. The case was about the latest version of a data compression library project called XZ Utilis, which was already ready for distribution on millions of Linux devices around the world. If the backdoor had not been noticed, the impact would not have been limited to Linux users, but it would have been possible that harm would have been experienced outside the Linux product family as well. The analysis of exactly what was to be done with the back door is still ongoing. However, it is known that this was an extremely critical vulnerability targeting the encrypted communication protocol (SSH). The nature of open source does not involve standardized audits or quality control processes, but the quality of the code is controlled by all its developers. In this case the vulnerability was discovered by a single security expert who tried the beta version of the project's latest update in his spare time. By chance, he noticed that there was something in the code that he initially suspected to be a bug, but later revealed to be a vulnerability that had been purposefully left there.

XZ Utilis is an open-source project that has been going on for years, which means that practically anyone interested has been able to participate in the development of the application. However, this does not mean that anyone would have been be able to add the now-detected backdoor to its latest versions. By analyzing the code, it has been possible to see that this was not an accident, but that an individual developer has systematically and deliberately built the backdoor for a reason that is still unknown at the moment. It was also not a low level participant of the project, but a reputable developer who had been working on it for several years and had reached a leading position. The developer, who goes by the name JiaT75 or Jia Tan, was practically acting as the second leader of the project, who through years of work had reached a position where he had the rights to make changes to the application without having to confirm them separately by anyone.

Looking at JiaT75's rise to a leading position, it has been found that some of the project member accounts that highlighted his abilities and trustworthiness may have been fake. In addition, the developer itself had recently contacted several parties to ensure that they deployed the latest version of the application (i.e. with a backdoor) as quickly as possible. As noted, there is no exact information as to why all this was done. It is not even known whether the JiaT75 worked alone or whether there was a larger group behind the same profile. Suspicions have been directed at both organised crime and state actors. For criminals, this kind of vulnerability could have been an extremely valuable trade product, while for state actors it would have provided opportunities for effective intelligence gathering around the world. It is also possible that it was really just a "lone wolf" who, for some reason, decided to build a back door to millions of devices. Part of the problem is how little is known about this developer, who has contributed the project significantly over the years. It underscores the risks associated with open-source projects.

There are also many benefits associated with using open source. Again, this vulnerability might not have been discovered if it had not been for the open-source system that anyone can view. However, it is worth raising questions. In practice, how can volunteer semi-anonymous individuals be involved in developing solutions that affect devices around the world without anyone outside of these projects being obliged to inspect them for errors or deliberate backdoors? It is not possible to say exactly how long it would have taken to detect the vulnerability in this case. If there hadn't been a small bug in the back door that affected the operation of one of the tester's devices, no one would necessarily have had a reason to start going through its latest changes. It is not possible to know whether it would have taken days, weeks or even years to detect the vulnerability. Organizations using open-source solutions need to understand not only the benefits but also the risks that open development brings. Especially in large-scale projects, auditing can be laborious, and if, for example, the end product combines several openly developed code libraries, it can be very difficult to find out who has ultimately produced the content for it. At best, open-source solutions can be more secure and error-free than closed solutions, because their development may have been influenced by several competent factors. At worst, even one skilled operator can pose a significant risk.

EXPLOITATION OF ZERO-DAY VULNERABILITIES ON THE RISE

Zero-day vulnerabilities are perhaps the single most serious security threat. Simply put, a zero-day vulnerability refers to an unknown security vulnerability in an application or system. These vulnerabilities are often only revealed when the malicious actor who discovered them exploits them to commit a data breach or other crime. The name zero day refers to how much time a defender (whether it's the developer or user of an app) has to react to a threat once it's revealed. Zero-day attacks have a high success rate, and knowledge of them is a valuable commodity for those planning crimes. These vulnerabilities are sought and patched by security researchers and bug hunters, while threat actors seek to find and exploit them.

The exploitation of zero-day vulnerabilities has been on the rise for several years. Google's threat intelligence group TAG (Threat Analysis Group) and security company Mandiant published a joint report on zero-day vulnerabilities discovered last year at the turn of March and April. A total of 97 zero-day attacks were detected in 2023, more than in 2022 (62) but fewer than in the peak year of 2021 (106). Also interesting is the profile of actors exploiting zero-day vulnerabilities. According to the report, 41.4% of the actors exploiting them in 2023 were commercial spyware, 41.4% were identified state actors and the remaining 17% were financially motivated criminals. Commercial spyware refers to spyware developed by private companies, such as the high-profile Pegasus and Predator malware. Of the state actors, China is the most active actor identified.

Recent trends in zero-day vulnerabilities have included attacks on software providers and their products used in the business world. Cybercriminals have discovered the value of vulnerabilites in these actors' applications, which is highlighted by the continuous expansion of application subcontracting chains. Especially various security applications are popular with criminals because they are usually trusted a lot, which also makes security vulnerabilities valuable. Lately, instead of global data giants, attention has focused on smaller, but still hundreds of organizations, application providers and their solutions. Of course, flaws in the products of major application developers, such as Google, Apple and Microsoft, are also of interest to criminals. However, applications from larger vendors are being developed by a larger number of personnel and undergo more detailed audit processes, making it much harder to find vulnerabilities in them. In practice, criminals have found that it is usually easier to find zero-day solutions in the products of smaller application developers

than in the solutions of global data giants, and they can still expose tens, hundreds or even thousands of organizations with a single attack. Last year, for example, we remember the attack of the Russian Cl0p ransomware group targeting the MOVEit data transfer application of the US company Progress Software, in which thousands of organisations around the world were victims and tens of millions of individuals affected.

Another notable example from last year is the attack on another US app provider, Barracuda Networks. In this attack linked to Chinese state actors, a zero-day vulnerability discovered in Barracuda's Email Security Gateway (ESG) product, which increases the security of email transmission, the threat actor was able to infect dozens of companies and government entities across multiple continents with email-intercepting malware. It is noteworthy not only that the Chinese managed to keep their activities secret for several months, but also that the attack was so serious and advanced that Barracuda saw fit to physically replace some of the exposed network equipment with new ones. According to the company, it was otherwise not possible to guarantee that the threat actor would be deported without leaving him with a back door to the systems.

Zero-day attacks therefore present challenges in terms of prevention, detection and recovery. However, it is not impossible to prepare for the threat. Organizations need to understand that application providers who produce solutions for many companies are becoming increasingly interested. Even if these suppliers do everything they can, there is always a chance that a motivated and resourced threat actor will find a zero-day vulnerability. Preparedness emphasises that organizations need to consider what data will be processed with which application and what is the backup solution if a certain product stops working. For example, in the case of the previously mentioned MOVEit attack, many victims were able to immediately establish that they were not dealing with a serious threat when they knew exactly what data had been processed with the application in question and that nothing critical had ended up in the hands of the threat actor. The worse situation was for those who had used this application produced by a third party to transfer sensitive data, and worst, for those who did not even know what data it had processed.

THE SECURITY RISKS OF A PUBLIC WI-FI NETWORK ARE ALWAYS TOPICAL

The temptation to use a public Wi-Fi network can be great, for example, when traveling for work or leisure. However, there are security risks associated with public Wi-Fi networks that one should at least be aware of. Although the threat itself is not new, it is worth recalling the basics of cybersecurity. At worst, sensitive data, such as usernames and passwords, may end up in the hands of threat actors, or through a public network, the threat actor may manage to break deeper into the user's systems. When operating in a public place, other information security risks are also emphasized. These threats include, for example, physical snooping on data/screens or the loss or theft of devices.

The greatest risk of public Wi-Fi networks manifests itself in the fact that the network owner has a view of all data traffic that takes place on the network and is transmitted through it. In some cases, malicious actors using the same network can also intercept (so called "sniffing attack") the public network with the help of applications developed for it. In particular, this enables the collection and further utilisation of unencrypted data circulating online. The threat can also be realized through the so-called "Evil Twin" attack method. This simply means a fake network created by criminals, where criminals create Wi-Fi names that sound appropriate in themselves, such as the name of a city or a service such as a café or library, but actually use the network to steal the information that moves through it. When connecting and surfing in a public network, special attention should be paid to the reliability of the network provider. Another problem may be the update rate of public networks or the level of security, which is difficult for the average user to figure out.

There may also be infected devices or hackers lurking on the public network. Often when joining a new network environment, the device may ask about sharing data with other devices on the same network. Under no circumstances should this be allowed, as it could lead, for example, to the spread of malware over the network. Man-in-the-middle attacks in public networks are also common, where the threat actor places itself unnoticed between the device connecting to the network and the network, which in practice guarantees access to all data traffic between them. The most common way to break into a network is that still many operators offering public Wi-Fi ś have not changed the settings of the network modem received from the operator, which makes it possible to log in with admin credentials found on the internet and change the network settings for anyone.

However, there are several ways to avoid and protect from public Wi-Fi security threats. The best way to prevent risks from materializing is to avoid using public Wi-Fi networks or at least refrain from using the most sensitive information, such as online banking credentials, in public places. At the company level, it is the management's responsibility to provide instructions on whether public Wi-Fi networks can be used on work computers and, if so, what issues can be dealt with. Visits to only secure https websites that encrypt communications also serve as a way to reduce risks. However, this does not deprive cybercriminals of the possibility of intercepting encrypted traffic and attempting to decrypt it, which may become possible in the future, for example as quantum technology advances and enables the decryption of existing encryption methods. One widely recommended method by security professionals to protect from the risks of public Wi-Fi connections is to use VPNs, as a VPN connection protects all traffic between your device and the VPN server. However, this creates a new threat scenario, as the data ends up to the VPN provider instead of the public network owner.

REFERENCES:

WHO IS RESPONSIBLE FOR OPEN SOURCE SECURITY

https://seclists.org/oss-sec/2024/q1/268

https://theintercept.com/2024/04/03/linux-hack-xz-utils-backdoor/

https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/

https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27

https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/

https://www.tivi.fi/uutiset/vakava-tietoturva-aukko-paljastui-vahingossa-suomalaisen-kehittamaan-projektiin-oli-ujutettu-takaportti/788cdb5e-d1a3-4321-a57a-7a7a40cc6700

https://www.theverge.com/2024/4/2/24119342/xz-utils-linux-backdoor-attempt?showComments=1

EXPLOITATION OF ZERO-DAY VULNERABILITIES ON THE RISE

https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business

https://www.techtarget.com/searchsecurity/news/366564654/Another-Barracuda-ESG-zero-day-flaw-exploited-in-the-wild

https://www.theregister.com/2024/03/27/surge_in_enterprise_zero_days/

https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

THE SECURITY RISKS OF A PUBLIC WI-FI NETWORK ARE ALWAYS TOPICAL

https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

https://www.f-secure.com/fi/articles/is-public-wi-fi-safe

https://www.forbes.com/advisor/business/public-wifi-risks/

Cyberwatch Weekly

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Pixabay
Unsplash

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi