



Trends and Challenges in Cyber Security

Quarterly Assessment, 3rd Quarter 2021

Critical Vulnerability in Confluence Affected Three Estonian State Agencies

SITUATION

On 25 August, software vendor Atlassian announced a critical vulnerability (CVE-2021-26084) in their Confluence Server and Data Centre software and asked customers to update them. Confluence is a popular wiki software that is used in both the public and private sectors in Estonia. The intranets of enterprises and institutions are often based on it.

The security vulnerability allowed an unauthenticated user to compromise the Confluence server of an enterprise or institution and edit, add, delete, and/or copy data there. In addition, it allowed malicious code to be installed on the systems of the victim to mine cryptocurrency or create a backdoor to return later and carry out new attacks. Atlassian rated the severity of these vulnerabilities on a ten-point scale with a near-maximum 9.8.

After the vulnerability had been disclo-

sed, several cyber groups and individual hackers began searching the Internet for servers that used outdated or vulnerable versions of Confluence.

Some were also found in Estonia and among other victims, the attackers managed to compromise the intranets of three Estonian state agencies.

ASSESSMENT

There is nothing new about critical vulnerabilities being found in software. However, the time between the disclosure of vulnerabilities and the attacks exploiting them is getting shorter. On 3 September, cybersecurity firm Bad Packets announced that it had identified the scanning and abuse of the Confluence security vulnerability in Russia, Hong Kong, Brazil, Nepal, Poland, Romania, Estonia, the United States, and Italy.

As the attackers get faster, so must the defenders. Unfortunately, a week and a half

after the security patches were released, we detected a number of servers in Estonia where the old version of Confluence was still used. Critical security updates must be installed as soon as possible, as each delayed minute increases the likelihood that the attacker will be successful. Therefore, the relevant notifications and warnings issued by CERT-EE should always be addressed as soon as possible.

As a second recommendation, it is worth considering whether the internal services of an enterprise or institution, such as the intranet built on Confluence, should be available on the public Internet or only from the internal network of the institution, which can be accessed via a secure VPN.

Thanks to the early detection of the attackers, there was no remarkable damage to the three state agencies affected, but following the above recommendations could have prevented these incidents from happening at all.

Legacy Systems Affect Both Public and Private Sectors

SITUATION

Last summer, there were two notable incidents in the services of the Information System Authority (RIA). The first was the case of the access rights management system (AAR). It was discovered that on the entrepreneur page of the state portal (while logged in), one could find a database in the AAR self-service environment with 336,733 data lines, where the given name and surname, personal identification code, connection with the enterprise/institution, and the position of the person could be seen.

The access rights management system had been built years ago in such a way that the data of authorised persons were also visible to other authorised persons. At the time, the approach to data protection and privacy was much less strict than it is today. Thus, it was high time to update the system and fix this issue.

The Information System Authority had to learn another lesson just a few weeks la-

ter, when CERT-EE discovered that 286,438 photographs of identity documents had been illegally downloaded from the identity document database. This was possible due to a security vulnerability in the so-called photo service, which did not properly verify the origin of the certificate created by the attacker.

ASSESSMENT

Despite the timing and similar scale, there is no direct link between the two cases. However, both incidents point to the same problem – outdated systems or legacy. Namely, both the access rights management system AAR and the photo service are part of the so-called legacy of the Information System Authority.

Legacy is a system, technology, or software that is still running but is actually outdated and becoming more and more vulnerable over time. For example, the current owners of a system developed 10 years ago may not have a full understanding of its structure and functions. Organisations change

over time, people are replaced, and often, the solutions that were once put in place have not even been properly documented. Therefore, it is often hard to predict what effect an upgrade of one part may have on another part of the system.

Outdated systems still in use can be found in both the public and private sectors. In many respects this is understandable: replacing the legacy is costly and time-consuming and can also lead to a change in the familiar functionalities.

What can be done to improve the situation? The first step is to get to know the legacy of your enterprise or institution. This gives you an idea of the state of the system, what features it offers (some of them may not be needed anymore), and what are the most critical issues. This allows you to assess which risks need to be addressed first and which may need to be accepted. In addition, a thorough knowledge of the old system and its weaknesses is a good starting point for developing a new one.

Cryptocurrency Fraud Schemes On The Rise

SITUATION

In the last three months, we received several reports from individuals about various cryptocurrency schemes. Among these were two more costly cases: one victim lost almost 16,000 euros and another 10,000 euros. In both cases, the fraudsters persuaded the person to make transactions on a cryptocurrency trading platform from which the money could not be withdrawn later.

The fraudsters approach their victims in different ways: in some cases, it starts with a phone call offering a lucrative investment opportunity, in other cases, the person falls victim to false advertising on social media. In one of the above-mentioned cases, the victim met a foreigner on Facebook Dating who offered the opportunity to earn money by investing in cryptocurrency by following his tips.

In September, we also saw a wave of phishing emails notifying the recipient that their 'bitcoin balance' contained a certain amount of money and the person had to 'verify' their account in order to receive it. The purpose of the phishing was to obtain the data of their actual bank account. There were also cases where fraudsters claimed that the person had made a very profitable investment in cryptocurrency and now, they had to pay commission or make a transfer of the same amount from their regular bank account to get their money.

ASSESSMENT

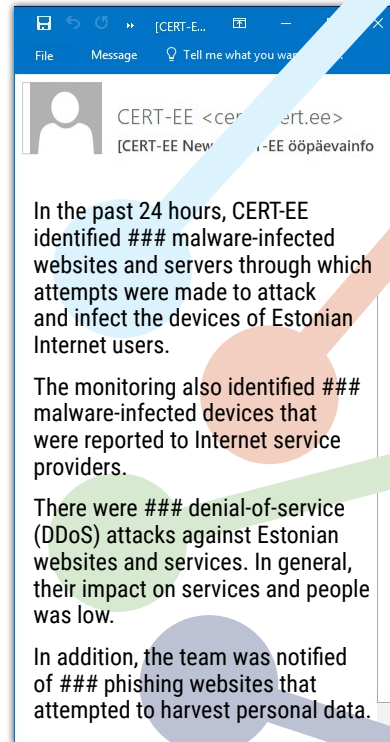
Financial fraud against individuals is an increasing problem in Estonia. In addition to fraudulent calls imitating banks, fraud schemes related to cryptocurrencies have also proliferated in recent months, and we expect that trend to continue. The regulation related to cryptocurrencies is still evolving and it is difficult for law enforcement agencies to track the movement of cryptocurrencies. Furthermore, the fact that the value of the most well-known cryptocurrency, bitcoin, has multiplied over the last year also works in favour of fraudsters: people are more inclined to believe in these earning opportunities.

What can you do to protect yourself from fraud? Be extremely sceptical about any investment opportunities offered by strangers over the phone or on social media, do not allow yourself to be influenced by fake pages that seem to prove high returns or by pressure to make a decision as soon as possible, do not respond to threats ('If you do not pay us more, you will lose everything.'). Background research should be done anyway, but in some cases it may not give accurate results as fake environments are constantly being created and closed. Anyone can be targeted by fraudsters, and the best way to protect ourselves is to increase awareness – talk to your family members and senior relatives about these types of scams.

24 Hours in Cyberspace: Infections, Attacks, and Vulnerabilities

CERT-EE has been producing a daily newsletter (in Estonian) that summarises cyber and IT news from public sources for many years. The newsletter contains references to news published in both Estonian and international media.

Since September, the newsletter also includes a brief overview of the situation in the Estonian cyberspace. Below is an explanation of what the statistics and data in the overview mean.



At the end of the newsletter, some specific incident involving fraud, compromise, ransomware, or other malware is often described. To subscribe to the newsletter (in Estonian), send an email with the subject 'Subscribe' to certnews@cert.ee.

CERT-EE detects such websites and servers during its daily monitoring of cyberspace. This autumn, the malware used is usually Mirai. We share this information with Internet service providers, web hosts, or various anti-virus software vendors who have the ability to directly combat these attacks.

These malware-infected devices are detected by our international partners (private companies, research institutes, and industry-specific non-profit organisations) who scan the entire Internet for malware and security vulnerabilities. We automatically forward the information to network owners (such as Internet service providers or enterprises).

We usually find out about low-impact DDoS attacks through our international partners that use specific tools. If a DDoS attack has higher impact, we are usually notified by the affected organisation or institution.

CERT-EE is notified directly of phishing websites if someone accidentally enters the site. The CERT-EE team will then contact the site host to take down the website. CERT-EE also provides information on phishing websites to various partners (CERTs from other countries, cyber community information sharing environments, etc.). We also provide information on larger phishing campaigns on CERT-EE Twitter and on RIA's Facebook page.

GOING WELL: ↗

TalTech with the support of Startup Estonia will launch the project 'Women in cyber security – role models for girls', which aims to encourage more girls and women to work in the field of IT and cyber security. The project introduces inspiring women who are working in the field, provides the necessary teaching materials for schools, and promotes community interaction. Read [more about the project here](#).

COULD BE IMPROVED: ⚠

For more than two years, CERT-EE has been sending data to telecommunications companies, web service providers, and network administrators on the number of infections or vulnerabilities in their networks. Unfortunately, these notifications are very often not forwarded to the end users that might benefit from them. Contact your internet service provider if you suspect you have not received important information about vulnerabilities and infections in your network.

This summary was prepared by the Cyber Security Branch of the Estonian Information System Authority (RIA) with the aim of explaining the trends of cyber threats to the widest possible audience, including readers outside Estonia. The situation in cyberspace is analysed in more detail in monthly summaries. CERT-EE distributes more technical recommendations at trainings and on RIA's website.