Part 1. Software Security

Martin Pavlinov Zhelev

CMP417: Engineering Resilient Systems

BSc (Hons) Ethical Hacking Year 4

2023/2024

Note that Information contained in this document is for educational purposes.

Contents

1 CONTEXT

ScottishGlen is a small energy company. In response to comments made by the CEO a hacktivist group, angered by the comments, has been sending threatening messages to employees. The CEO has tasked the IT manager for ScottishGlen to improve the security posture of the company to ensure it is more resilient to attacks from technical and human perspective.

To improve the security of the company the IT manager decided to focus on the Kerberos network authentication system used by ScottishGlen, since it could potentially be exploited by a malicious actor which could lead to various security risks such as unauthorized access, data theft, impersonation etc.

1.1 KERBEROS

Kerberos was developed in the Massachusetts Institute of Technology (MIT) in the early 1980s and has been the default authentication method in Windows since 2000. Moreover, it is also built into all major operating systems such as Apple macOS, FreeBSD and Linux (Loshin, n.d.). The latest version of it is Version 5 Release 1.21.2, which was released on 14th of August 2023. It is a protocol for ensure secure communications across an untrusted network. A common use for it is to allow single sign-on (SSO) which lets users securely access different systems and services with one username and password. (IBM, 2021)

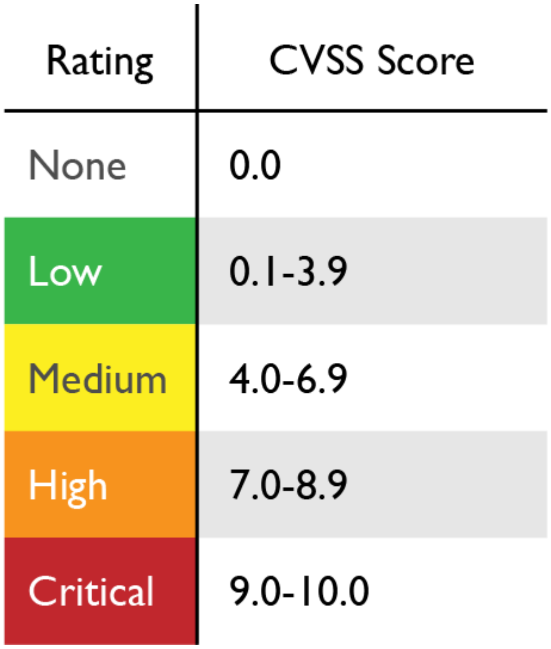
Because of its popularity, significance and age, the Kerberos protocol is being evaluated extensively by cyber security researchers which had led to the discovery of a lot of security vulnerabilities. These vulnerabilities can be found in the Common Vulnerabilities and Exposures (CVE) database.

1.2 CVE DATABASE

The Common Vulnerabilities and Exposures (CVE) is a free publicly available database that is ran by the MITRE corporation and is sponsored by the US government. It Is commonly used by organisation and cyber security professionals to track security issues.

In the CVE database every CVE is given a unique number which has the following format CVE-YEAR-SEQUENTIALNUMBER as well as description of the issue, versions of software it affects, solutions and its severity. (Balbix, n.d.)

Each CVE is also given a Common Vulnerability Scoring System (CVSS) score to determine its severity. CVSS scores can be a value from 0 to 10 and depend on variety of factors such as the ease of executing the attack, privileges required etc. (Figure 1) (Risto, 2023)



Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 1: CVSS Scores (Benq, 2020)

1.3 BUFFER BOUND VULNERABILITIES

As of writing this, Kerberos has 312 vulnerabilities out of which thirty-eight were caused because of buffer bound vulnerabilities such as buffer overflows and over-reads. These vulnerabilities are a major threat to the integrity of Kerberos systems and need to always be patched to prevent their existence on a system. (MITRE, n.d.)

Buffer bound vulnerabilities are caused by faulty written code that goes over the bound of a “buffer,” because it does not have proper input validation and memory management. (Urquhart, 2023)

A buffer is a region in memory used to temporally store memory before it is processed. During a buffer overflow attack malicious code is written outside of its intended area into an area a buffer intended for code that is about to be executed. This in turn can lead severe consequences such as arbitrary code execution, data corruption or a crash. (Figure 2) (OWASP Foundation, n.d.)

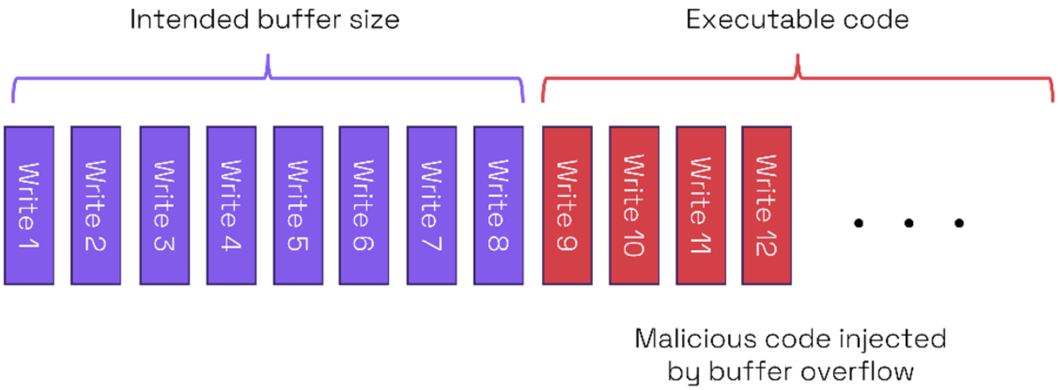


Figure 2: Buffer overflow example. (Urquhart, 2023)

A buffer over-read is the opposite of an overflow. While a buffer overflow involves writing outside the intended buffer, a buffer over-read the program reads outside its intended buffer. This unintended access to adjacent memory buffer could allow it to access a buffer containing confidential data. (Figure 2) (Urquhart, 2023)

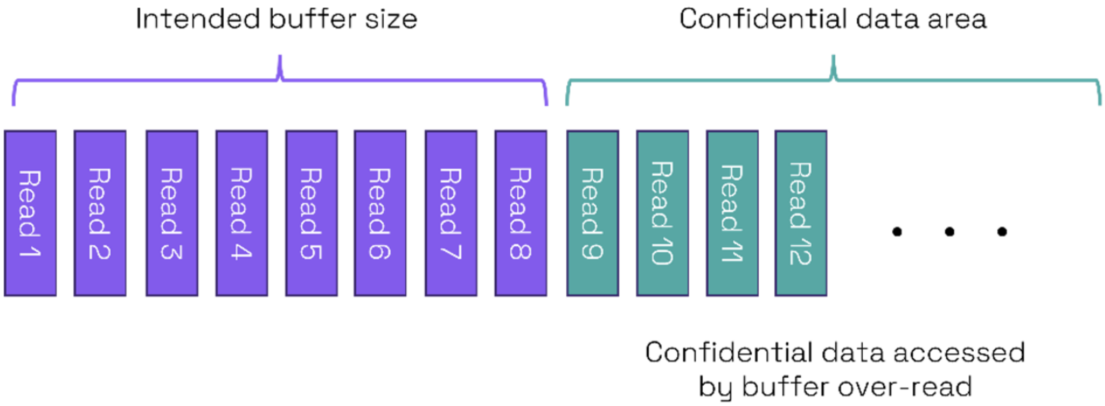


Figure 3: Buffer over-read example. (Urquhart, 2023).

A famous buffer overflow attack was the computer worm called SQL Slammer. It utilised a vulnerability in Microsoft SQL Server 2000 and MSDE 2000 Hosts that was given the CVE number - CVE-2002-0649. (F-Secure, n.d.) The worm would use the buffer overflow vulnerability to self-propagate which allowed it to infect around 75 000 machines worldwide. Because of its rapid spread and significant impact, it increased the IT world's cyber security vigilance (Kristoff, 2023)

Kerberos is written in C, which means it is more susceptible to buffer bound vulnerabilities. This is because the C programming language has low level access to memory using pointers, but also completely lacks automatic memory management. The lack of safeguards means that the likelihood of buffer bound vulnerabilities existing is significantly increased especially if if code is not written carefully and does not follow Secure Coding Practices. (Rathi, 2023)

2 RECOMMENDATION

In this section of the report the researcher will explain what secure coding practices are, discuss their significance for software development and how they can prevent various cyber security threats such as buffer overflow attacks.

2.1 SECURE CODING PRACTICES

Building secure applications is extremely important for a company's cyber resilience. To build a secure application developers should follow a guide such as the Secure Coding practices guide by the OWASP Federation, which provides a Secure Coding Practices Checklist that helps ensure no important practices are missed during development. "Generally, it is much less expensive to build secure software than to correct security issues after the software package has been completed, not to mention the costs that may be associated with a security breach." (OWASP Foundation, 2010). In the case of the Kerberos implementation for ScottishGlen secure coding practices of high priority should be the ones on input validation and memory management.

2.2 INPUT VALIDATION

Input validation is the practice of validating that the input is only data of certain type, length, and content. It is important for the ScottishGlen team to focus on and implement, because by ensuring only properly formatted data is accepted into forms, they will be able to reduce the likelihood of buffer bound vulnerabilities. (OWASP Foundation, 2010)

2.3 MEMORY MANAGEMENT

Memory management is another practice that should be heavily focused on, because as discussed earlier Kerberos is written in C and code written in low level languages such as C and C++ is more vulnerable to buffer bound vulnerabilities if secure coding practices are not followed. (Rathi, 2023)

2.4 CODE REVIEW

Finally, code review should be performed regularly and thoroughly to ensure all developers are up to date with the current code base. By ensuring frequent code review is part of the development process, the software engineers are going to be able to detect and fix bugs earlier in development, which would improve the overall quality of the project.

It should be noted that while this report identifies these three practices of upmost importance that does not mean that the rest of the Secure Coding Practices in the OWASP Framework guide should be ignored and deemed unnecessary.

3 IMPLEMENTATION

As previously discussed, the vulnerability type that Kerberos is most vulnerable to is buffer bound vulnerabilities. These vulnerabilities, including buffer overflow and buffer over-read are big threats to the cyber resilience of Kerberos systems. In this section the latest buffer overflow vulnerability affecting Kerberos will be explained followed by how it can be prevented by ensuring secure coding practices are followed.

3.1 CVE-2022-42898

The latest vulnerability affected Kerberos has been given the unique CVE number CVE-2022-42898 and has CVSS score of 8.8 - High. The link to the CVE description can be found in Section 5 - References. It affects Kerberos 5 before 1.19.4 and 1.20.x before 1.20.1 (MITRE, 2022). This vulnerability involves integer overflow that can cause a remote code execution attack on 32-bit platforms and a denial of service (DDoS) attack on other platforms. (Hudson, 2022)

It is caused by an issue in its “krb5_parse_pac()” function that can make it overflow during header and memory length calculations. The trigger for this error is providing a serialised PAC file with a buffer count of 2^28 or higher (Hudson, 2022)

3.2 PREVENTION

Using the Secure Coding Practices Guide from OWASP (OWASP Foundation, 2010) the possibility of this vulnerability occurring will be significantly reduced. Firstly, by implementing proper input validation it will be no longer possible to provide a PAC file with the required buffer count. Alongside this if such a file does end up getting provided exception handling can be implemented to detect the malicious PAC file and stop the program from executing further until non malicious PAC file is provided.

Secondly, with proper memory management the developers will be able to make sure that the ”krb5_parse_pac” function’s buffer that gets created is of the right size and cannot be overflowed.

Finally, by having code review be a crucial part of the development process, the developers will be able to have the ability to spend more time reviewing each other’s code for potential vulnerabilities. The review process would also allow the creation of fresh ideas to solve certain coding challenges more effectively during development. By collaborating, the developer team will also be able to share experiences and improve each other’s knowledge.

In conclusion, by adhering to the Secure Coding Practice guide by the OWASP Foundation the software of ScottishGlen can be made less vulnerable as well as more resilient, because of the continues development and collaboration between the developers.

4 SUMMARY

To ensure that ScottishGlen is protected from potential cyber attacks the Kerberos network authentication system should be analysed and secured, because of its age and popularity. This is because the Kerberos system, which is commonly used for single sign on (SSO) implementations, has had a considerable number of vulnerabilities discovered particularly of the buffer bound vulnerability type such as buffer overflows and buffer over-reads.

Kerberos is written in C which has a low-level access to memory using pointers, but also completely lacks automatic memory management. Because of the lack of safeguards in C, to reduce the chances of writing faulty code that is susceptible to buffer bound vulnerabilities, the team should follow the input validation and memory management checklist in the secure coding practices guide from the OWASP Foundation (OWASP Foundation, 2010). This should help mitigate the threat of such vulnerabilities occurring.

Alongside this the team should also focus on implementing effective and thorough code review process, which would not only further decrease the risk of vulnerabilities being present in the code but would also improve the overall quality of the project and foster knowledge sharing between team members.

5 REFERENCES

Balbix, n.d. *What is a CVE?.* [Online]
Available at: https://www.balbix.com/insights/what-is-a-cve/
[Accessed 14 February 2024].

Benq, 2020. *What is CVE and CVSS.* [Online]
Available at: https://www.benq.com/en-in/business/resource/trends/what-is-cve-and-cvss.html
[Accessed 14 February 2024].

F-Secure, n.d. *Worm:W32/Slammer.* [Online]
Available at: https://www.f-secure.com/v-descs/mssqlm.shtml
[Accessed 14 February 2024].

Hudson, G., 2022. *MITKRB5-SA-2022-001 Vulnerabilities in PAC parsing.* [Online]
Available at: https://mailman.mit.edu/pipermail/kerberos-announce/2022q4/000202.html
[Accessed 17 February 2024].

IBM, 2021. *Introduction to Kerberos.* [Online]
Available at: https://www.ibm.com/docs/en/streams/4.2.0?topic=authentication-introduction-kerberos
[Accessed 13 February 2024].

Kristoff, J., 2023. *Remembering SQL Slammer.* [Online]
Available at: https://www.netscout.com/blog/asert/remembering-sql-slammer
[Accessed 14 February 2024].

Loshin, P., n.d. *What is Kerberos and How Does It Work.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/Kerberos
[Accessed 13 February 2024].

MITRE, 2022. *CVE-2022-42898.* [Online]
Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42898
[Accessed 16 February 2024].

MITRE, n.d. *CVE-Search Results.* [Online]
Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=kerberos
[Accessed 14 February 2024].

OWASP Foundation, 2010. *Secure Coding Practices - Quick Start Guide.* [Online]
Available at: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf
[Accessed 14 February 2023].

OWASP Foundation, n.d. *Buffer Overlow | OWASP Foundation.* [Online]
Available at: https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
[Accessed 14 February 2024].

Rathi, A., 2023. *C Programming Language Standard.* [Online]
Available at: https://www.geeksforgeeks.org/c-programming-language-standard/
[Accessed 15 February 2023].

Risto, J., 2023. *What is Common Vulnerability Scoring System (CVSS).* [Online]
Available at: https://www.sans.org/blog/what-is-cvss/
[Accessed 14 February 2024].

Urquhart, R., 2023. *Buffer bound vulnerabilities and their dangers.* [Online]
Available at: https://codasip.com/2023/10/20/buffer-bound-vulnerabilities-and-their-dangers/
[Accessed 14 February 2024].