Part 1: Software Security

ScottishGlen Case Study

Marc Geggan

CMP417: Engineering Resilient Systems

2022/23

Word count: 1950

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

Abstract

ScottishGlen has tasked the author with undertaking a security posture assessment of their company to investigate potential vulnerabilities within their deployed applications and systems. This request has been prompted by recent threats made to the company from a hacktivist group. It was acknowledged that their **Kerberos Network Authentication System** should be selected for security review. The researcher has identified three vulnerabilities: **CVE-2022-33647**, **CVE-2021-42287**, and **CVE-2020-3125**. This report will analyse these vulnerabilities, and then provide effective prevention techniques that should be implemented to eliminate the threat of the reported CVEs. The class of security fault that the CVEs fall under has been identified as **improper authentication**. The suggested secure software development practice is to implement **multi-factor authentication (MFA)**. It has been described within this report how this implementation will effectively reduce the risk of analysed CVEs, and how the recommended practice will change how developers are working. It is important to note that these implementations are not a final solution to defend from cyber-attacks and further work should be undertaken by appropriate teams.

+Contents

1 INTRODUCTION

This paper will discuss possible vulnerabilities within the companies' systems and applications and provide mitigations against them. The researcher has selected the Kerberos Network Authentication System for security review as it handles the client/server communications for the company and if exploited could give the hacktivist group unrestricted access to the network.

1.1 KERBEROS

Kerberos, a network authentication protocol, is designed to provide strong authentication for client/server applications by adopting secret-key cryptography methods *(MIT, 2019)*. The authentication protocol was developed by Massachusetts Institute of Technology (MIT) and has become an industry standard protocol for network authentication. The protocol was named Kerberos after a Greek mythology, a three headed dog. The three heads of the Kerberos protocol present:

- The client or principal.
- The network resource, which is the application server that provides access to the network resource.
- The key distribution centre (KDC), a third-party authentication service.

Services using Kerberos only need to trust the KDC, as it runs as a single service providing both an authentication service and ticket granting service *(techtarget.com, n.d.).*

The authentication process consists of the following steps:

1. The client logs in and requests the TGT from the AS.
2. The KDC verifies the client's credentials and sends an encrypted session key and TGT.
3. The client decrypts the message, generates an authenticator, and sends a request for access to the TGS.
4. The TGS creates a ticket for the file server and generates a shared service session key for the target server and client.
5. The client decrypts the file ticket and generates another authenticator, which is sent to the target server along with the service ticket.
6. The target server decrypts the service ticket and extracts the session key.
7. The server and the client have authenticated each other.

Kerberos is such a widely used authentication protocol, meaning it is not invulnerable and has been the target for many hackers. There have been multiple ways developed to hack Kerberos such as forged tickets, encryption downgrading malware, and password guessing *(Fortinet, n.d.)*.

2 COMMON VULNERABILITIES AND EXPOSURES

CVE, or Common Vulnerabilities and Exposures, is a project that aims to provide a standardized way of identifying and classifying security vulnerabilities in software. Each vulnerability is assigned a unique CVE number and a CVSS score, which measures the severity of the vulnerability. The CVE number is comprised of three parts: "CVE", the year of disclosure, and an identifier assigned by a CVE Numbering Authority (CNA).

There are various types of vulnerabilities, each with their distinct characteristics and modes of exploitation. In the case of Kerberos authentication protocol, some potential vulnerabilities include **Kerberoasting**, **AS-REP Roasting**, and **Golden Tickets**. These vulnerabilities can result in an attacker gaining unauthorized access to sensitive data, impersonating legitimate users, or causing Denial of Service (DoS) attacks. It is important to address these vulnerabilities promptly to prevent any potential harm to the system.

2.1 CVE-2022-33647

This **privilege elevation and improper authentication** vulnerability has a CVSS score of **8.1**, making it a **high severity** if exploited. It affects sixteen versions of Windows Server from 2008 to 2022 *(NIST, 2022)*, and there has been a technical analysis of this CVE published online.

The vulnerability is a type of **AS-REP Roasting** attack and can be exploited by attackers who have gained a 'Man-In-The-Middle' attack foothold between the client and domain controller. The pre-authentication method is also used in this exploit, as it is enabled by default for every Active Directory object. This method allows an attacker to modify KDC pre-auth response as there is **no verification** at that authentication stage. The exploit also forces the client to downgrade the encryption to MD4-RC4, which is vulnerable to attack *(Lellin, 2022)*. Once the encryption has been downgraded, the attacker can crack the targets cypher key. If this vulnerability was exploited, an attacker could compromise the users Kerberos session key to elevate themselves to SYSTEM privileges and gain unrestricted access to the systems *(MSRC, 2022)*.

2.2 CVE-2021-42287

This **security bypass** vulnerability has a CVSS score of **8.8**, making it a **high severity** if exploited. It affects eighteen versions of Windows Server from 2008 to 2022 *(NIST, 2021)* and there has been documentation on exploitation posted online, with Fortinet posting a guide on gaining domain admin by combining CVE-2021-42287 and CVE-2021-42278, and PoC code posted on sites such as GitHub *(Yavo, 2022).*

The exploit targets the Kerberos Privilege Attribute Certificate (PAC) and involves impersonating domain controllers. A compromised account can cause the KDC to create a service ticket with higher privileges making it harder for the KDC to identify which account the ticket is for *(Microsoft, 2021)*. Attackers can combine this CVE with CVE-2021-42278 to easily **elevate the privileges** to Domain Admin within the active directory after compromising any regular user in the domain *(CalCom, 2022).*

2.3 CVE-2020-3125

This **improper authentication** vulnerability has a CVSS score of **8.1**, making it a **high severity** if exploited. It affects the Cisco Adaptive Security Appliance (ADA) which contains a weakness that could permit a remote attacker to impersonate the Kerberos key distribution center (KDC) and gain access to an affected device that is configured for VPN or local device access without proper authentication.

The vulnerability arises from insufficient identity verification of the KDC following a successful authentication response *(CVE, 2020).* An attacker could exploit this vulnerability by spoofing the KDC server response to the ASA device. Since the KDC does not authenticate this malicious response, it could successfully bypass Kerberos authentication and allow a remote attacker to gain access. The only things the attacker would need is an authorized username, and a spoofed Kerberos domain controller *(Cisco, 2020).*

3 CLASS OF SECURITY FAULT

3.1 IMPROPER AUTHENTICATION

All the previously mentioned CVEs were exploited on the Kerberos software through some form of improper authentication. This class of security fault occurs when an attacker is able to gain access to the target system or application without proper authentication ore authorization. It can arise from a variety of issues such as lack of authentication within certain services, exploitable weak authentication mechanisms, or even human error in software code. Malicious threat actors would exploit this fault for many reasons, including gaining access to sensitive data, stealing confidential information, or executing malicious actions within the system such as active directory domain takeovers.

One common fault classed under improper authentication is lack of verification within an application. This occurs when applications do not properly verify the identity of users before granting access to sensitive resources. Attackers can exploit this by impersonating legitimate users or by using stolen credentials to gain access to sensitive data. Unauthenticated responses between client and server can also be exploited by attackers.

Another common fault classed under improper authentication is the ability to bypass authentication. This can be exploited if the application has weak authentication mechanisms, or an attacker is able to confuse the service. Unauthenticated responses from authentication services can also be exploited. By utilizing Man-In-The-Middle attacks for example, attackers can capture a request from server and reply with their own data, which would be accepted if the server did not authenticate the origin of responses.

Exploiting improper authentication on Kerberos can lead to severe consequences such as privilege escalation, unauthorized access to sensitive data, and complete control of the system. Attackers can use various methods such as bypassing authentication, lack of verification, and unauthenticated responses to gain access to systems and elevate their privileges. It is essential to address these vulnerabilities promptly to prevent potential security breaches.

4 SECURE SOFTWARE DEV RECOMMENDATIONS

4.1 DEFENSE IN DEPTH (MULTI-FACTOR AUTHENTICATION)

Multi-factor authentication (MFA) is a method of authentication that requires a client or end user to provide two or more verification factors to gain access to resources, applications, or systems. MFA is recognized as a core identity and access management policy as it requires more than just a username or password, decreasing the chances of a cyber-attack *(OneLogin, 2019)*. The additional factor could be something they know such as a pin code, something they have such as a token or smart card, or something they are such as biometrics. It can prevent many of the common attack methods used by threat actors and is a relatively simple and cost-effective security measure that can greatly reduce the risk of unauthorized access to sensitive information.

If the engineers at ScottishGlen implemented MFA across the company for all staff, all the CVE's risks analysed in the previous section would be greatly reduced. In the case of CVE-2022-33647, the attacker that gained a MITM foothold on the network would not be able to escalate their privileges to SYSTEM as they would need to provide additional authentication methods to access the targeted account, making it harder to exploit the vulnerability.

Similarly, MFA would prevent a threat actor from impersonating domain controllers and gaining access to the key distribution center (KDC) in CVE-2021-42287. The attacker would be required to provide additional authentication factors for gaining access, making it much harder to impersonate the domain controller and exploit the vulnerability.

Finally, in the case of CVE-2020-3125, multi-factor authentication would prevent a remote attacker from impersonating the KDC and gaining access to an affected device. The attacker would need to provide multiple authentication factors, thus making it much harder to spoof the KDC server response and bypass authentication.

Implementing MFA across the company will change how the developers are working as it requires careful planning and consideration of factors within the business, and specific needs and requirements of people and applications. To implement it, the developers should first assess their current architecture and determine which services are critical and require MFA. Then they will need to ensure all services and applications they operate on will support MFA. Next, they should ensure MFA is enforced for all authentication attempts between client and server, meaning all clients must provide a secondary form of authentication in addition to a password. It is important to note that the passwords of clients and services must also adhere to strict password policies. Developers will also be required to educate the staff within ScottishGlen on how to properly use and configure MFA to ensure it remains effective. Finally, the developers will be required to regularly monitor and update the MFA implementation. This would involve periodically reviewing logs and alerts and implementing further security controls such as whitelisting access from clients to services or requiring additional authentication for sensitive systems or services.

References

MIT (2019). *Kerberos: The Network Authentication Protocol*. [online] Mit.edu. Available at: https://web.mit.edu/kerberos/.

SearchSecurity. (n.d.). *What is Kerberos and How Does it Work? - Definition from SearchSecurity*. [online] Available at: https://www.techtarget.com/searchsecurity/definition/Kerberos.

Fortinet. (n.d.). *What Is Kerberos? Kerberos Authentication Explained*. [online] Available at: https://www.fortinet.com/resources/cyberglossary/kerberos-authentication.

nvd.nist.gov. (2022). *NVD - CVE-2022-33647*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2022-33647#match-8326741

Iellin, D.S., Yoav (2022). *Technical Analysis of Kerberos Vulnerabilities*. [online] Silverfort. Available at: https://www.silverfort.com/blog/technical-analysis-of-cve-2022-33679-and-cve-2022-33647-kerberos-vulnerabilities/

msrc.microsoft.com. (n.d.). *Security Update Guide - Microsoft Security Response Center*. [online] Available at: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-33647

cve.mitre.org. (2020). *CVE - CVE-2020-3125*. [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3125 [Accessed 14 Mar. 2023].

Cisco Security Advisory (2020) *Cisco Adaptive Security Appliance Software Kerberos Authentication Bypass Vulnerability*. Available at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-asa-kerberos-bypass-96Gghe2sS

Yavo, U. (2022). *From User to Domain Admin in (less than) 60 seconds: CVE-2021-42278/CVE-2021-42287 | FortiGuard Labs*. [online] Fortinet Blog. Available at: https://www.fortinet.com/blog/threat-research/cve-2021-42278-cve-2021-42287-from-user-to-domain-admin-60-seconds#:~:text=The%20combination%20of%20CVE%2D2021

support.microsoft.com. (2021). *KB5008380—Authentication updates (CVE-2021-42287)*. [online] Available at: https://support.microsoft.com/en-gb/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041.

CalCom. (2022). *CVE-2021-42278 SAM & CVE-2021-42287 KDC vulnerability*. [online] Available at: https://www.calcomsoftware.com/cve-2021-42278-sam-cve-2021-42287-kdc-vulnerability/

OneLogin (2019). *What is Multi-Factor Authentication (MFA), and how does it work?* [online] OneLogin. Available at: https://www.onelogin.com/learn/what-is-mfa.