CAS Authentication Timing Attack

1. Summary

The Client Access Server (CAS) that services Autodiscover and Outlook Web App (OWA) has been found to be vulnerable to time-based authentication attacks. It has been discovered that when sending authentication requests to the CAS, behavior in the timing of the responses can be used to verify Active Directory (AD) realms and usernames within those realms. Authentication timing issues have been found in specific IIS file paths and OWA form-based authentication. This issue can allow an attacker to confirm the existence of a specific username in the directory, and will make other attacks such as password guessing or social engineering attacks more successful.

2. Description

When analyzing the response times of authentication requests, there is a noticeable time delay between realms and usernames that exist or don't exist. It is believed that the underlying issues exists in Windows Kerberos. When the CAS sends authentication requests to the domain controller (KDC) the pre-authentication process is staged in such a way that noticeable time delays exist. OWA form-based authentication and IIS file paths were found vulnerable to this timing delay. The services and authentication paths that have been found vulnerable can be seen below in Table 1.

TABLE 1—VULNERABLE SERVICES

SERVICE	AUTHENTICATION PATH
Exchange Autodiscover 2013	/Autodiscover/Autodiscover.xml
Exchange OWA 2013	Form Based Authentication
Exchange Autodiscover 2010	/Autodiscover/Autodiscover.xml
Exchange OWA 2010	Form Based Authentication
Exchange OWA 2010/Forefront TMG 2010	/EWS/Exchange.asmx
Exchange OWA 2010/Forefront TMG 2010	Form Based Authentication
Exchange OWA 2007	Form Based Authentication

During the testing of the IIS file paths, HTTP NTLM authentication requests were being used. Typically, the realm name, username, and password is required for authentication. There is a case where the CAS can be configured so that the realm name isn't required and authentication can be accomplished with just a username and password. In this case, the realm name doesn't need to be known and usernames can be enumerated.

Table 2 below details the Windows Kerberos process and approximate response times seen when sending requests to vulnerable services. It should be noted that system resources and network configurations can play a role in response time variations seen. During authentication, when the realm exists but the username doesn't exist, these times can vary from system to system but the resulting time response is the same average time. For example, it has been seen on a OWA/Forefront TMG

2010 setup that when sending authentication requests to the EWS path, every authentication request will take approximately 60 seconds to respond. When sending form-based authentication requests to OWA 2013, every authentication request can take approximately 15 seconds to respond but another system running the same configuration with more system resources could take approximately 5 seconds to respond. As seen above, the response times in different environments may have different response times but the pattern in the timing response behavior patterns still exist.

TABLE 2—WINDOWS KERBEROS REVIEW

AUTHENTICATION REQUEST	KERBEROS PROCESS	RESPONSE TIME
Non-existing realm	KDC searches for realm	2-3 seconds
Realm exists but username doesn't exist	Pre-authentication ticket created to verify username	5-60 seconds (varies but a pattern exists)
Realm and username exists	Pre-authentication ticket created to verify password	<2 seconds

- **Non-existing realm** - It has been seen that when a non-existing realm names are being tested, that the first request takes 2-3 seconds, and then all requests thereafter take less than one second. What is believed to be happening here is that the first request is searching for the realm and fails but the search response is cached on the CAS for 30 seconds. Thus, the 2-3 second response is seen every 30 seconds.
- **Realm exists but username doesn't exist** - A pre-authentication ticket is created to verify the username exists in the realm. The average time of the request can vary depending on resources but the resulting time response is consistent. This could be either approximately 5 seconds or higher. The highest response time seen is approximately 60 seconds.
- **Realm and username exists** - A pre-authentication ticket is created to verify the password. The time in seconds has been seen to take less then 2 seconds but in most cases this response time is under one second.

Table 3 below details an example of the timing attack analysis. This test was completed against a fully patched Exchange 2013 environment running Windows 2008 R2 server. The OWA 2013 form-based authentication response times were being monitored. The domain *CORP* is a valid realm and the usernames *user_exist_1*, *user_exist_2,* and *user_exist_3* are valid account names.

TABLE 3—TIMING ATTACK ANALYSIS

#	TIME (SECONDS)	REALM	USERNAME
1	2.261	ACME	doesnt_exist_1
2	0.011	ACME	doesnt_exist_2
3	5.222	CORP	doesnt_exist_3
4	0.239	CORP	user_exist_1
5	0.259	CORP	user_exist_2
6	5.430	CORP	doesnt_exist_4
7	5.636	CORP	doesnt_exist_5
8	0.236	CORP	user_exist_3

The results are described below.

- **Non-existing realm** - This can be seen in response # 1 and 2.
- **Realm exists but username doesn't exist** - This can be seen in response # 3, 6, and 7.
- **Realm and username exists** - This can be seen in response # 4, 5, and 8.

3. Impact

The issues detailed allow an attacker to enumerate AD realms and usernames which could lead to further compromise. There are many ways to identify realms and username formats, such as searching public databases, stripping metadata from published documents, by reviewing SMTP mail headers and services, or even by obtaining wordlists of the top most popular first and last names and creating a list of correctly formatted usernames to try with a brute force attack. The impact should be categorized as an information disclosure vulnerability.

4. Affected Products

Microsoft Exchange CAS 2013

Microsoft Exchange CAS 2010

Microsoft Exchange CAS 2010/Forefront TMG 2010

Microsoft Exchange CAS 2007

5. Time Line

02/14/2014 Reported Vulnerability to the Vendor

03/10/2014 Vendor Confirmed the Vulnerability

08/01/2014 Publicly Disclosed

6. Credits

Discovered by Nate Power