Autodiscover Enumeration Vulnerability

1. Summary

The Microsoft Exchange Client Access Server (CAS) that services Autodiscover has been found vulnerable to an information disclosure. It has been discovered that a standard domain user without Exchange permissions can enumerate Autodiscover configuration files of Exchange users by an XML SOAP parameter injection.

This issue can allow an attacker to confirm the existence of a specific email addresses. The type of information that is disclosed are things such as, legacy accounts and their username formats. The end user's full name is also revealed which could aid in locating a user's account. Exchange services, permissions, and the location of the domain controller that handles authentication are revealed as well.

2. Description

Autodiscover is a CAS service that is used to configure remote or internal mail clients for use with Exchange systems. Using a compatible mail client, the user can configure their client by providing an email address and password. The mail client goes through a discovery process to locate the remote CAS server hosting the Autodiscover configuration file. The configuration file is hosted on an IIS web server. By default the configuration file path is "/Autodiscover/Autodiscover.xml".

To access the Autodiscover.xml configuration file, an XML SOAP request is sent to the server using an HTTP POST method. Server side application controls require the User-Agent header of the request must represent that of an Outlook client, such as "Microsoft Office/12.0". The body of the SOAP request can be seen in Figure 1.

Figure 1—XML SOAP Request Body

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/
requestschema/2006">

<Request>

<EMailAddress>jsmith@example.com</EMailAddress>

<AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscover/outlook/
responseschema/2006">

</AcceptableResponseSchema>

</Request>

</Autodiscover>
```

By examining the body of the SOAP request made, it was found that modifying the "EmailAddress" parameter to utilize another existing email address, the user's configuration data can be enumerated.

Using a single set of valid credentials, it is possible to inject the “EmailAddress” parameter to discover valid email addresses and gather data about the users and the environment. It was also found that even though valid Active Directory credentials are required to access the Autodiscover.xml file, it is not required to be a valid Exchange account with mailbox permissions.

There are many ways to build an email address list that can be used when injecting the “EmailAddress” parameter, 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 email addresses to try with this enumeration attack.

3. Impact

Allows an attacker to enumerate Exchange user and environment information which could lead to further compromise such as password guessing attacks, social engineering, and learning about internal systems. The impact should be categorized as an information disclosure vulnerability.

4. Affected Products

Microsoft Exchange CAS 2013

Microsoft Exchange CAS 2010

Microsoft Exchange CAS 2007

5. Time Line

05/27/2014 Reported Vulnerability to the Vendor

06/26/2014 Vendor Confirmed the Vulnerability

08/01/2014 Publicly Disclosed

6. Credits

Discovered by Nate Power