Exchange Multiple Internal IP Disclosures

1. Summary

Multiple issues have been discovered that makes it possible to disclose internal IP addresses of remote Microsoft Exchange environments. This includes internal addresses of the Client Access Server (CAS) which hosts services such as Outlook Web App (OWA) and Autodiscover. This also includes internal addresses of the proxy or gateways processing requests for the OWA.

2. Description

Attack #1 - OWA / Autodiscover

When sending a crafted GET requests to the web server with empty host header and using the HTTP protocol version 1.0(HTTP/1.0), the internal IP addresses of the under lying system is revealed in the header response. This flaw is believed to be an IIS issue and has been found in Microsoft Exchange systems such as Outlook Web App (OWA) and the Client Access Server (CAS). The flaw has been seen in Basic Authentication response headers on a 401 web server status and the Location headers on a 302 web server status. It's possible this flaw exists in other products that run on IIS.

An example of normal behavior can be seen when performing a HTTP/1.1 request to a protected page such as:

```
"https://autodiscover.example.com/Autodiscover/Autodiscover.xml"
```

The Basic Authentication HTTP header response normally reveals a public facing IP address or hostname of:

```
WWW-Authenticate: Basic realm="autodiscover.example.com"
```

A proof of concept example can be seen below in Figure 1. All the vulnerable IIS paths discovered and there affected product versions can be seen in Table 1. Note that some of the file paths disclosed are vulnerable if default settings have not been changed. Some of the paths have been found vulnerable based on system administrator changes.

TABLE 1—VULNERABLE PATHS

SERVICE	STATUS	VULNERABLE HEADER	IIS PATHS
Autodiscover	401	Basic Authentication	/Autodiscover/ /Autodiscover/Autodiscover.xml
ActiveSync	401	Basic Authentication	/Microsoft-Server-ActiveSync /Microsoft-Server-ActiveSync/default.eas

SERVICE	STATUS	VULNERABLE HEADER	IIS PATHS
OWA	302, 401	Location, Basic Authentication	/ECP /EWS /EWS/Exchange.asmx /Exchange /OWA

FIGURE 1—BASIC AUTH HEADER REVEALS INTERNAL IP ADDRESS

```
$ openssl s_client -host autodiscover.example.com -port 443

---SNIP---

GET /Autodiscover/Autodiscover.xml HTTP/1.0


HTTP/1.1 401 Unauthorized

Cache-Control: private

Content-Type: text/html

Server: Microsoft-IIS/7.5

X-SOAP-Enabled: True

X-WSSecurity-Enabled: True

X-WSSecurity-For: None

X-AspNet-Version: 2.0.50727

WWW-Authenticate: Negotiate

WWW-Authenticate: NTLM

WWW-Authenticate: Basic realm="10.1.1.10"

X-Powered-By: ASP.NET

---SNIP---
```

Attack #2 - Reverse Proxy / Gateway

It has been shown in OWA 2007 and 2010, that it's possible to reveal the internal IP address of the reverse proxy or gateway processing requests for OWA. Such proxies or gateways include Forefront TMG 2010.

This attack can be performed using a web browser. When attempting to trigger ASP.NET debug and making a GET request to the OWA path "/owa/auth/trace.axd". The OWA throws a server side exception with a web server status of 403. The verbose error reveals the internal IP address of the proxy or gateway. An example of this output can be seen below in Figure 2.

FIGURE 2—REVERSE PROXY/GATEWAY INTERNAL IP DISCLOSED

```
An error occurred and your request couldn't be completed. If the problem continues,
contact your helpdesk with this HTTP Status code: 403.

Request
```

```
Url: https://mail.example.com/owa/auth/trace.axd

User host address: 10.1.1.1

OWA version: 14.2.318.3
```

3. Impact

Allow an attacker to gather information about the internal network.

4. Affected Products

Microsoft Exchange CAS 2013

Microsoft Exchange CAS 2010

Microsoft Exchange CAS 2010/Forefront TMG 2010

Microsoft Exchange CAS 2007

Microsoft Exchange OWA 2003

5. Solution

Only attack two is fixed in current versions. Apply the latest supplied vendor patches.

6. Time Line

12/17/2012 Reported Vulnerability to the Vendor

1/03/2013 Vendor Confirmed the Vulnerability

08/01/2014 Publicly Disclosed

7. Credits

Discovered by Nate Power