

[NT] Considerations for IIS Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0029.html>

From: support@securiteam.com

Date: 03/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 6 Mar 2002 11:51:26 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Considerations for IIS Authentication

SUMMARY

Microsoft's Internet Information Server offers Web, FTP, Mail and NNTP services. It is possible to force the web service to authenticate a user even if anonymous access is allowed to the resource being requested. This may open three low risk vulnerabilities on the server -- two problems with information leakage and the possibility to perform brute force attacks against system user accounts.

DETAILS

IIS supports anonymous access, Basic authentication and Integrated Windows authentication using NTLM. By making a request to the web server offering credentials the web server will attempt to authenticate the user. If authentication fails the server responds with a 401 Access Denied message. Depending upon what forms of authentication have been disabled or left enabled different actions can be performed.

To ascertain if the server supports Basic Authentication one would make a request with the following Authorization header:

```
GET / HTTP/1.1
```

```
Host: iis-server
```

```
Authorization: Basic cTFraTk6ZDA5a2xt
```

Securiteam: [NT] Considerations for IIS Authentication

If the server responds with a 401 Access Denied response then Basic auth is enabled. If the server responds with a 200 OK then this means one of two things – the server does not support Basic auth (the most likely) or there is a system account on the server called "q1ki9" with a password of "d09klm" (most unlikely!).

To ascertain if the server supports NTLM Authentication one would make a request with the following Authorization header:

```
GET / HTTP/1.1
```

```
Host: iis-server
```

```
Authorization: Negotiate TIRMTVNTUAAABAAAAB4IAoAAAAAAAAAAAAAAAAAAAAA=
```

Again if the server responds with a 401 Access Denied message then the server supports NTLM auth. If a 200 OK response is returned then the server does not support Integrated Windows authentication.

Provided at least one authentication method is supported an attacker can mount a brute force attack against system accounts. More than likely the default "administrator" account would be the target as normally this account can't be locked out and is highly privileged.

In terms of information leakage, if Basic auth is supported when making a request whatever is entered in the client Host HTTP header is used as the Realm. The Realm information is served by the server to the client so the client can tell when it should or shouldn't present authentication credentials. If the Host header field is left blank the server will, by default, use its IP address as the Realm. If the server is protected by a firewall that employs Network Address Translation and has a private IP address such as 10.x.x.x then this will be returned to the client. This information can aid an attacker when formulating other attacks.

If NTLM authentication is supported then it is possible to discover the NetBIOS name of the server and the Windows NT domain it resides in. This information is returned as Base64 encoded text in response to a client Authorization request.

Fix information:

If the server is intended for public use then it may be possible to simply disable both Basic and Integrated Windows authentication. Sites that use forms based logins, for example when users are authenticated against a database, and track logged in users with cookies will be able to disable these authentication methods. Doing this will prevent such attacks.

If Basic or Integrated Windows authentication are required then it is possible to mitigate the risk.

Setting account lockout will help minimize the risk of successful brute force attacks. Using the "passprop" utility it is possible to enable account lockout for the default "administrator" account.

Securiteam: [NT] Considerations for IIS Authentication

One should also seriously consider renaming this administrator account if this has not already been done.

To prevent internal IP address disclosure take the following steps.

Open a command prompt and change the current directory to

c:\inetpub\adminscripts or to where the adminscripts can be found.

Run the commands

```
adsutil set w3svc/UseHostName True
net stop iisadmin /y
net start w3svc
```

This will cause the IIS server to use the machine's host name rather than its IP address.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nisr@NEXTGENSS.COM> David Litchfield.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] mod_ssl Buffer Overflow Condition (Patch Available)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)