IIS5.1 Directory Authentication Bypass by using ":$I30:$Index_Allocation"

IIS5.1 Directory Authentication Bypass by using ":$I30:$Index_Allocation" - Soroush Dalili, soroush.me.

- Published: date not stated
- Original: <https://soroush.me/blog/iis5-1-directory-authentication-bypass-by-using-i30index-allocation>
- Preserved from: https://soroush.me/blog/iis5-1-directory-authentication-bypass-by-using-i30index-allocation (stored) on 2026-08-11
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

IIS5.1 Directory Authentication Bypass by using ":$I30:$Index_Allocation"

Download this advisory from: http://soroush.secproject.com/downloadable/IIS5.1_Authentication_Bypass.pdf or: http://0me.me/demo/IIS/IIS5.1_Authentication_Bypass.pdf

Description: Although IIS5 is very old, finding one is not impossible! Therefore, I want to introduce a technique to bypass the IIS authentication methods on a directory. This vulnerability is because of using Alternate Data Stream to open a protected folder. All of IIS authentication methods can be circumvented. In this technique, we can add a ":$i30:$INDEX_ALLOCATION" to a directory name to bypass the authentication. In a protected folder such as "AuthNeeded" which includes "secretfile.asp": It is possible to run "secretfile.asp" by using: "/AuthNeeded:$i30:$INDEX_ALLOCATION/secretfile.asp" Instead of: "/AuthNeeded/secretfile.asp"

More description: ***Why IIS6 and 7 are not vulnerable:*** – In these versions, IIS does not accept colon (":") character from the URL before the querystring.

Why we cannot use "::$Data" in IIS 5.1 anymore: – IIS rejects the request if its URL contains "::$" (before querystring).

Why IIS5 is vulnerable to "Directory Authentication Bypass" by using ":$I30:$Index_Allocation": – IIS only verifies the directory name to check for authentication. Therefore, we can use "http://victim.com/SecretFolder:$I30:$Index_Allocation/" instead of "http://victim.com/SecretFolder" to bypass the authentication.

Is it possible to bypass something else by using ":$I30:$Index_Allocation" on a NTFS partition: – If a checking is only based on the directory name, it can be bypassed by using this method.

Download this advisory from: http://soroush.secproject.com/downloadable/IIS5.1_Authentication_Bypass.pdf or: http://0me.me/demo/IIS/IIS5.1_Authentication_Bypass.pdf

This entry was posted in Security Posts

Creation date: July 1, 2010

Previous New update – July 2010[

Next

Opera Browser – Scroll Information Leakage