

Microsoft IIS - Short File/Folder Name Disclosure



EDB-ID:
19525

EDB Verified:
✓

CVE:

EDB Verified:

Author:
SOROUSH DALILI



Exploit:  / 

Type:
WEBAPPS

Platform:
WINDOWS

Date:
2012-07-02

Vulnerable App:





This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only

Allow all cookies

Show details ▼

Website : http://soroush.secproject.com/blog/

I. BACKGROUND

"IIS is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. IIS is the third most popular server in the world." (Wikipedia)

II. DESCRIPTION

Vulnerability Research Team discovered a vulnerability in Microsoft IIS.

The vulnerability is caused by a tilde character "~" in a Get request, which could allow remote attackers to diclose File and Folder names.

III. AFFECTED PRODUCTS

- IIS 1.0, Windows NT 3.51
- IIS 2.0, Windows NT 4.0
- IIS 3.0, Windows NT 4.0 Service Pack 2
- IIS 4.0, Windows NT 4.0 Option Pack
- IIS 5.0, Windows 2000
- IIS 5.1, Windows XP Professional and Windows XP Media Center Edition
- IIS 6.0, Windows Server 2003 and Windows XP Professional x64 Edition
- IIS 7.0, Windows Server 2008 and Windows Vista
- IIS 7.5, Windows 7 (error remotely enabled or no web.config)