



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 

Microsoft IIS - Short File/Folder Name Disclosure



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 

Platform:

WINDOWS

Date:

2012-07-02

Vulnerable App:



PoC: <https://gitlab.com/exploit-database/exploitdb-bin-spl0its/-/raw/main/bin-spl0its/19525.zip>

Paper: <http://www.exploit-db.com/docs/19527.pdf>



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 ▼

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)
IIS 7.5, Windows 2008 (classic pipeline mode)

Note: Does not work when IIS uses .Net Framework 4.



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 ▼

<http://soroush.secproject.com/blog/2012/06/microsoft-iis-tilde-character-vulnerabilityfeature-short-filefolder-name-disclosure/>

V. SOLUTION

There are still workarounds through Vendor and security vendors.
Using a configured WAF may be usefull (discarding web requests including the tilde "~" character).

VI. CREDIT

This vulnerability was discovered by:

Soroush Dalili (@irsdl)
Ali Abbasnejad

VII. REFERENCES

<http://support.microsoft.com/kb/142982/en-us>
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation/

VIII. DISCLOSURE TIMELINE

2010-08-01 - Vulnerability Discovered
2010-08-03 - Vendor Informed
2010-12-01 - Vendor 1st Response
2011-01-04 - Vendor 2nd Response (next version fix)
2012-06-29 - Public Disclosure

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

© OffSec

[Services](#)

[Limited](#)

2024. All rights reserved.