master 1 branch 0 tags Go to file Add file Code

edwardz246003 Update exploit.py 1 153460c on 27 Mar 2017 6 commits

README.md	Update README.md	5 years ago
exploit.py	Update exploit.py	5 years ago

README.md

CVE-2017-7269

[Description] Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.

[Additional Information] the ScStoragePathFromUrl function is called twice

[Vulnerability Type] Buffer overflow

[Vendor of Product] Microsoft

[Affected Product Code Base] Windows Server 2003 R2

[Affected Component] ScStoragePathFromUrl

[Attack Type] Remote

[Impact Code execution] true

[Attack Vectors] crafted PROPFIND data

[Has vendor confirmed or acknowledged the vulnerability?] true

[Discoverer] Zhiniang Peng and Chen Wu.

Information Security Lab & School of Computer Science & Engineering, South China University of Technology Guangzhou, China

About

Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.

Readme
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

Python 100.0%