1. Out-of-date Version (IIS)

HIGH | 1

Netsparker identified the target web site is using IIS and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Internet Information Services Other Vulnerability

** DISPUTED ** Microsoft Internet Information Services (IIS), when accessed through a TCP connection with a large window size, allows remote attackers to cause a denial of service (network bandwidth consumption) via a Range header that specifies multiple copies of the same fragment. NOTE: the severity of this issue has been disputed by third parties, who state that the large window size required by the attack is not normally supported or configured by the server, or that a DDoS-style attack would accomplish the same goal.

Affected Versions

10.0

External References

- CVE-2007-0087

Internet Information Services Other Vulnerability

Denial of service in Windows NT IIS server using ..\..

Affected Versions

10.0

External References

- CVE-1999-0229

Internet Information Services Other Vulnerability

IIS allows local users to cause a denial of service via invalid regular expressions in a Visual Basic script in an ASP page.

Affected Versions

10.0

External References

- CVE-2000-0115

Vulnerabilities

1.1. http://livingdonorportal.com/portal-admin/patient-directory

Identified Version

- 10.0

Latest Version

- 10.0 (in this branch)

Vulnerability Database

- Result is based on 03/25/2021 11:00:00 vulnerability database content.

Certainty

Request

```
GET https://www.livingdonorportal.com/portal-admin/patient-directory HTTP/1.1
Origin: https://www.livingdonorportal.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
Sec-Fetch-User: ?1
Referer: https://www.livingdonorportal.com/
Cookie: ASP.NET_SessionId=cdf3zhoktpielz0ryxc2pfh2; CMSPreferredCulture=en-CA; .ASPXFORMSAUTH=CBE516
990AC28B452DAF630AF543B266894ACEC68F4F7FC2205721DF47EBF9D73EC250EE263503C4FD1D34DB4C4C4BB557ED69A2D1
7964FEA07F0535331455F11094F1BD4751A7CABFC1A017612F427C8C13A174FB4F86C9BE27134E827CC370C2E4AE55861436
2A524E0C168509CE39DEEB587924C9BE825DC8D617EA6E57AF; CMSPreferredUICulture=en-US; CMSViewMode=0
```

Response

Response Time (ms) : 0 **Total Bytes Received** : 64668 **Body Length** : 64340 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-UA-Compatible: IE=Edge
X-Frame-Options: SAMEORIGIN
Date: Tue, 30 Mar 2021 20:57:46 GMT
Cache-Control: private, no-store, must-revalidate
content-type: text/html; charset=utf-8
content-HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-UA-Compatible: IE=Edge
X-Frame-Options: SAMEORIGIN
Date: Tue, 30 Mar 2021 20:57:46 GMT
Cache-Control: private, no-store
…
```

Remedy

Upgrading IIS to a higher version is not a standalone operation. The IIS version depends heavily on the Windows OS version that you use on your server machine.

If it is not possible to upgrade IIS to a higher version for this type of reason, we strongly recommend that you track and apply the patches that are published by the vendor.

Please note that all updates and patches for IIS come as Windows Updates. Also, you can select which update package(s) will be applied.

External References

- The Official Microsoft IIS Site

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	937
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2