

## Exploit Arama Yöntemi

Herhangi bir sunucunun exploit'ini aramak istediğimizde google arama motoruna aşağıdaki anahtar kelimeler girilir

Google Arama Kutusu:

Windows Server 2016 exploits  
Windows Server 2012 exploits

...

Bu aramalar sonucunda CVE Details veritabanına götüren linke tıklanır.

[https://www.cvedetails.com/product/34965/Microsoft-Windows-Server-2016.html?vendor\\_id=26](https://www.cvedetails.com/product/34965/Microsoft-Windows-Server-2016.html?vendor_id=26)

[https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor\\_id=26](https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26)

...

CVEDetails veritabanında (örneğin yukarıdaki linklerden birinde) aşağıdaki gibi bir sayfa bizi karşılar.

The screenshot shows the CVE Details website for Microsoft Windows Server 2016. The page title is "Microsoft » Windows Server 2016 : Vulnerability Statistics". The main content area displays a table titled "Vulnerability Trends Over Time" with columns for Year, # of Vulnerabilities, DoS, Code Execution, Overflow, Memory Corruption, Sql Injection, XSS, Directory Traversal, Http Response Splitting, Bypass something, Gain Information, Gain Privileges, CSRF, File Inclusion, and # of exploits. Below the table are two bar charts: "Vulnerabilities By Year" and "Vulnerabilities By Type".

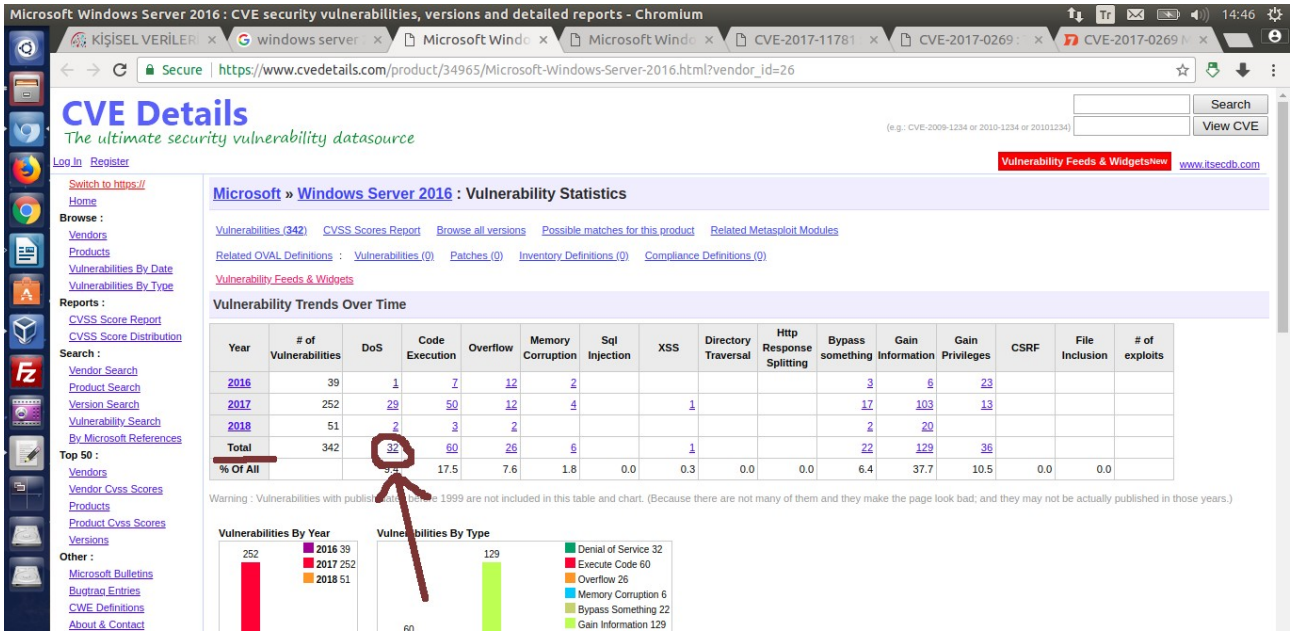
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2016	39	1	7	12	2					3	6	23			
2017	252	29	50	12	4		1			17	103	13			
2018	51	2	3	2						2	20				
Total	342	32	60	26	6		1			22	129	36			
% Of All		9.4	17.5	7.6	1.8	0.0	0.3	0.0	0.0	6.4	37.7	10.5	0.0	0.0	

Warning: Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year: 2016: 39, 2017: 252, 2018: 51

Vulnerabilities By Type: Denial of Service 32, Execute Code 60, Overflow 26, Memory Corruption 6, Bypass Something 22, Gain Information 129

Örneğin bu sayfada Window Server 2016'ya ait tüm zafiyetler kategorize edilerek sıralanmıştır. DoS, Code Execution, Overflow, ... vs. Bu zafiyetlerin altında ise satır satır yıllara göre çıkan zafiyetlerin sayısı gösterilmiştir. Total satırına gelip oradaki rakama tıkladığımızda (örn; DoS'un Total satırındaki rakama tıkladığımızda) Windows Server 2016'ya ait bu zamana kadar çıkmış tüm DoS zafiyetleri ekrana gelir.



Microsoft Windows Server 2016 : List of security vulnerabilities - Chromium

Secure | https://www.cvedetails.com/vulnerability-list/vendor\_id=26/product\_id=34965/opdos-1/Microsoft-Windows-Server-2016.html

## CVE Details

The ultimate security vulnerability datasource

Search [ ] View CVE

Vulnerability Feeds & Widgets [www.itsecdb.com](#)

### Microsoft » Windows Server 2016 : Security Vulnerabilities (Denial Of Service)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-0885	20		DoS	2018-03-14	2018-04-09	6.3	None	Remote	Medium	Single system	None	None	Complete
The Microsoft Hyper-V Network Switch in 64-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows a denial of service vulnerability due to how input from a privileged user on a guest operating system is validated, aka "Hyper-V Denial of Service Vulnerability".														
2	CVE-2018-0753	119		DoS Overflow	2018-01-04	2018-01-12	7.1	None	Remote	Medium	Not required	None	None	Complete
Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allow a denial of service vulnerability due to the way objects are handled in memory, aka "Windows IPsec Denial of Service Vulnerability".														
3	CVE-2017-11788	19		DoS	2017-11-14	2017-12-01	5.0	None	Remote	Low	Not required	None	None	Partial
Windows Search in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows server, version 1709 allows an unauthenticated attacker to remotely send specially crafted messages that could cause a denial of service against the system due to improperly handling objects in memory, aka "Windows Search Denial of Service Vulnerability".														
4	CVE-2017-11781	20		DoS	2017-10-13	2017-10-20	7.8	None	Remote	Low	Not required	None	None	Complete
The Microsoft Server Block Message (SMB) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a denial of service vulnerability when an attacker sends specially crafted requests to the server, aka "Windows SMB Denial of Service Vulnerability".														
5	CVE-2017-8704	20		DoS	2017-09-12	2017-09-21	4.9	None	Local	Low	Not required	None	None	Complete
The Windows Hyper-V component on Microsoft Windows 10 1607 and Windows Server 2016 allows a denial of service vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka "Hyper-V Denial of Service Vulnerability".														
6	CVE-2017-8623	20		DoS	2017-08-08	2017-08-14	6.8	None	Remote	Low	Single system	None	None	Complete
Windows Hyper-V in Windows 10 1607, 1703, and Windows Server 2016 allows a denial of service vulnerability when it fails to properly validate input from a privileged user on a guest operating system, aka "Windows Hyper-V Denial of Service Vulnerability".														
7	CVE-2017-8515	19		DoS	2017-06-14	2017-06-21	4.9	None	Local	Low	Not required	None	None	Complete
Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an unauthenticated attacker to send a specially crafted kernel mode request to cause a denial of service on the target system, aka "Windows VAD Cloning Denial of Service Vulnerability".														
8	CVE-2017-0280	20		DoS	2017-05-12	2018-03-27	7.1	None	Remote	Medium	Not required	None	None	Complete

Görüldüğü üzere Windows Server 2016 'nın DoS zafiyetlerini görüntülemekteyiz. Zafiyetlere sırasıyla tıkladığımızda aşağıdaki gibi bir sayfa bizi karşılar.



CVE-2017-11788 : Windows Search in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, - Chromium

https://www.cvedetails.com/cve/CVE-2017-11788/

CVSS Score **5.0**

Confidentiality Impact **None** (There is no impact to the confidentiality of the system.)

Integrity Impact **None** (There is no impact to the integrity of the system.)

Availability Impact **Partial** (There is reduced performance or interruptions in resource availability.)

Access Complexity **Low** (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication **Not required** (Authentication is not required to exploit the vulnerability.)

Gained Access **None**

Vulnerability Type(s) **Denial Of Service**

CWE ID **19**

**Products Affected By CVE-2017-11788**

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	OS	Microsoft	Windows 10	-			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
2	OS	Microsoft	Windows 10	1511			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
3	OS	Microsoft	Windows 10	1607			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
4	OS	Microsoft	Windows 10	1703			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
5	OS	Microsoft	Windows 10	1709			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
6	OS	Microsoft	Windows 7		SP1		<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
7	OS	Microsoft	Windows 8.1				<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
8	OS	Microsoft	Windows Rt 8.1				<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
9	OS	Microsoft	Windows Server	1709			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
10	OS	Microsoft	Windows Server 2008		SP2		<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
11	OS	Microsoft	Windows Server 2008	R2	SP1		<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
12	OS	Microsoft	Windows Server 2012	-			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
13	OS	Microsoft	Windows Server 2012	R2			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
14	OS	Microsoft	Windows Server 2016				<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>

**Number Of Affected Versions By Product**

Vendor	Product	Vulnerable Versions
Microsoft	Windows 10	1511, 1607, 1703, 1709
Microsoft	Windows 7	SP1
Microsoft	Windows 8.1	
Microsoft	Windows Rt 8.1	
Microsoft	Windows Server	1709
Microsoft	Windows Server 2008	SP2
Microsoft	Windows Server 2008	R2, SP1
Microsoft	Windows Server 2012	
Microsoft	Windows Server 2012	R2
Microsoft	Windows Server 2016	

Zafiyetin exploit edilebilmesi için authentication'ın gerekli olmayışı bizim avantajımızdır. Çünkü böylece credential'lara sahip olmadan exploitation yapabiliriz. Aşağıda exploitation yapmak için authentication'a ihtiyaç olmayan bir zafiyet gösterilmiştir.

CVE-2017-11788 : Windows Search in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, - Chromium

https://www.cvedetails.com/cve/CVE-2017-11788/

**CVE Details**  
The ultimate security vulnerability datasource

Vulnerability Details : **CVE-2017-11788**

Windows Search in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows server, version 1709 allows an unauthenticated attacker to remotely send specially crafted messages that could cause a denial of service against the system due to improperly handling objects in memory, aka "Windows Search Denial of Service Vulnerability".

Publish Date : 2017-11-14 Last Update Date : 2017-12-01

CVSS Scores & Vulnerability Types

CVSS Score **5.0**

Confidentiality Impact **None** (There is no impact to the confidentiality of the system.)

Integrity Impact **None** (There is no impact to the integrity of the system.)

Availability Impact **Partial** (There is reduced performance or interruptions in resource availability.)

Access Complexity **Low** (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication **Not required** (Authentication is not required to exploit the vulnerability.)

Gained Access **None**

Vulnerability Type(s) **Denial Of Service**

CWE ID **19**

**Products Affected By CVE-2017-11788**

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	OS	Microsoft	Windows 10	-			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
2	OS	Microsoft	Windows 10	1511			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>
3	OS	Microsoft	Windows 10	1607			<a href="#">Version Details</a> <a href="#">Vulnerabilities</a>

Seçtiğimiz zafiyet sayfasının en altında ise zafiyetin metasploit'te bir exploit modülüne sahip olup olmadığı bilgisi gösterilir

CVE-2017-11788 : Windows Search in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, - Chromium

https://www.cvedetails.com/cve/CVE-2017-11788/

Search By Microsoft Reference ID: (e.g.: ms10-001 or 979352)

OS	Microsoft	Windows Server 2008	R2	SP1	Version Details	Vulnerabilities
11	OS	Microsoft	Windows Server 2012	-	Version Details	Vulnerabilities
12	OS	Microsoft	Windows Server 2012	R2	Version Details	Vulnerabilities
13	OS	Microsoft	Windows Server 2016		Version Details	Vulnerabilities
14	OS	Microsoft	Windows Server 2016		Version Details	Vulnerabilities

- Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Windows 10	5
Microsoft	Windows 7	1
Microsoft	Windows 8.1	1
Microsoft	Windows Rt 8.1	1
Microsoft	Windows Server	1
Microsoft	Windows Server 2008	2
Microsoft	Windows Server 2012	2
Microsoft	Windows Server 2016	1

- References For CVE-2017-11788

<https://portal.mscc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11788> CONFIRM

<http://www.securitytracker.com/id/1039792>

SECTrack 1039792

<http://www.securityfocus.com/bid/101711>

BID 101711 Microsoft Windows Search CVE-2017-11788 Remote Denial of Service Vulnerability Release Date:2017-11-20

- Metasploit Modules Related To CVE-2017-11788

There are not any metasploit modules related to this CVE entry (Please visit [www.metasploit.com](http://www.metasploit.com) for more information)

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback

CVE is a registered trademark of the MITRE Corporation and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). CVE is a registered trademark of the MITRE Corporation and the authoritative source of OVAL content is [MITRE's OVAL web site](https://www.oval.org). OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is [MITRE's OVAL web site](https://www.oval.org). Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, service or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

Görüldüğü üzere seçtiğimiz zafiyetin metasploit'te bir modülü yokmuş. CVE Details veritabanının güncellenmemesi ihtimaline karşı google arama motoruna zafiyetin CVE kodunu (örneğin bu zafiyet için CVE-2017-11788 kodunu) girip rapid7 sitesinden metasploit modülü gelmiş mi (gösterilmekte mi) bakabiliriz.