

**TUGAS KEAMANAN JARINGAN KOMPUTER  
CVE PADA SISTEM OPERASI WINDOWS XP**



**Nama : Resti Handayani**

**Nim : 09011281419050**

**SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2018**

No	CVE ID	CWE ID	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-8487</a>	<a href="#">284</a>	Exec Code	2017-06-15	2017-08-11	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows OLE di Windows XP dan Windows Server 2003 memungkinkan penyerang untuk mengeksekusi kode saat korban membuka file atau program yang dibuat khusus alias "Windows olecnv32.dll Remote Code Execution Vulnerability.													
2	<a href="#">CVE-2017-8461</a>	<a href="#">284</a>	Exec Code	2017-06-15	2017-07-06	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
Windows RPC dengan Routing dan Remote Access yang diaktifkan pada Windows XP dan Windows Server 2003 memungkinkan penyerang untuk mengeksekusi kode pada server RPC yang ditargetkan yang memiliki Routing and Remote Access yang diaktifkan melalui aplikasi yang dibuat secara khusus, alias "Windows RPC Remote Code Execution Vulnerability."													
3	<a href="#">CVE-2017-0176</a>	<a href="#">284</a>	Exec Code Overflow	2017-06-22	2017-07-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Sebuah buffer overflow pada kode otentikasi Smart Card di gpkcsp.dll di Microsoft Windows XP melalui SP3 dan Server 2003 melalui SP2 memungkinkan penyerang remote untuk mengeksekusi kode sewenang-wenang pada komputer target, asalkan komputer tersebut tergabung dalam domain Windows dan memiliki Remote Desktop Konektivitas protokol (atau Terminal Services) diaktifkan													

[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	<a href="#">CVE-2017-8487</a>	<a href="#">284</a>		Exec Code	2017-06-15	2017-08-11	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows OLE in Windows XP and Windows Server 2003 allows an attacker to execute code when a victim opens a specially crafted file or program aka "Windows olecvt32.dll Remote Code Execution Vulnerability."														
2	<a href="#">CVE-2017-8461</a>	<a href="#">284</a>		Exec Code	2017-06-15	2017-07-06	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server which has Routing and Remote Access enabled via a specially crafted application, aka "Windows RPC Remote Code Execution Vulnerability."														
3	<a href="#">CVE-2017-0176</a>	<a href="#">284</a>		Exec Code Overflow	2017-06-22	2017-07-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.														
Total number of vulnerabilities : 3 Page : 1 (This Page)														

## Ranking

### Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#) [2014](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Linux Kernel</a>	<a href="#">Linux</a>	OS	<a href="#">2035</a>
2	<a href="#">Mac Os X</a>	<a href="#">Apple</a>	OS	<a href="#">1978</a>
3	<a href="#">Android</a>	<a href="#">Google</a>	OS	<a href="#">1607</a>
4	<a href="#">Chrome</a>	<a href="#">Google</a>	Application	<a href="#">1525</a>
5	<a href="#">Firefox</a>	<a href="#">Mozilla</a>	Application	<a href="#">1438</a>
6	<a href="#">Iphone Os</a>	<a href="#">Apple</a>	OS	<a href="#">1371</a>
7	<a href="#">Debian Linux</a>	<a href="#">Debian</a>	OS	<a href="#">1210</a>
8	<a href="#">Flash Player</a>	<a href="#">Adobe</a>	Application	<a href="#">1045</a>
9	<a href="#">Windows Server 2008</a>	<a href="#">Microsoft</a>	OS	<a href="#">1022</a>
10	<a href="#">Safari</a>	<a href="#">Apple</a>	Application	<a href="#">934</a>
11	<a href="#">Acrobat</a>	<a href="#">Adobe</a>	Application	<a href="#">909</a>
12	<a href="#">Internet Explorer</a>	<a href="#">Microsoft</a>	Application	<a href="#">905</a>
13	<a href="#">Ubuntu Linux</a>	<a href="#">Canonical</a>	OS	<a href="#">888</a>
14	<a href="#">Windows 7</a>	<a href="#">Microsoft</a>	OS	<a href="#">877</a>
15	<a href="#">Windows Vista</a>	<a href="#">Microsoft</a>	OS	<a href="#">816</a>
16	<a href="#">Opensuse</a>	<a href="#">Novell</a>	OS	<a href="#">784</a>
17	<a href="#">Windows Xp</a>	<a href="#">Microsoft</a>	OS	<a href="#">731</a>
18	<a href="#">Thunderbird</a>	<a href="#">Mozilla</a>	Application	<a href="#">703</a>
19	<a href="#">Seamonkey</a>	<a href="#">Mozilla</a>	Application	<a href="#">698</a>
20	<a href="#">Windows Server 2012</a>	<a href="#">Microsoft</a>	OS	<a href="#">650</a>
21	<a href="#">Acrobat Reader</a>	<a href="#">Adobe</a>	Application	<a href="#">643</a>
22	<a href="#">Mac Os X Server</a>	<a href="#">Apple</a>	OS	<a href="#">641</a>

Windows xp menempati peringkat ke-16 dalam situs resmi CVE  
(<https://www.cvedetails.com/top-50-products.php>)

## Hole

Pada versi terakhir update windows xp, hole yang dapat di jadikan target adalah windows xp melalui SP3 dan Server 2003 melalui SP2.