# Nove zakrpe za Microsoft proizvode 12/2010

U sklopu redovitog mjesečnog izdavanja zakrpi **Microsoft** je, u utorak 14. prosinca objavio 17 sigurnosnih zakrpi, od kojih su 2 klasificirane kao kritične, 14 kao važne i 1 kao relativno važna.

Preko servisa **windowsupdate.carnet.hr** na raspolaganju su zakrpe koje **Microsoft** opisuje u svome sigurnosnom *bulletinu* za prosinac 2010.g.:
http://www.microsoft.com/technet/security/bulletin/ms10-dec.mspx [1].

Zakrpe za prosinac ispravljaju slijedeće nedostatke:
**MS10-090** - Cumulative Security Update for Internet Explorer (2416400)
**MS10-091** - Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)
**MS10-092** - Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)
**MS10-093** - Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (2424434)
**MS10-094** - Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (2447961)
**MS10-095** - Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)
**MS10-096** - Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)
**MS10-097** - Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)
**MS10-098** - Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)
**MS10-099** - Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)
**MS10-100** - Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)
**MS10-101** - Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)
**MS10-102** - Vulnerability in Hyper-V Could Allow Denial of Service (2345316)
**MS10-103** - Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)
**MS10-104** - Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005)
**MS10-105** - Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)
**MS10-106** - Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132)

Servis **windowsupdate.carnet.hr** instaliran je u verziji **WSUS 3.0 SP2** čime su podržani novi serveri i klijenti:
- integracija sa **Windows Server 2008 R2**
- podrska za **BranchCache** servis u Windows Serveru 2008 R2
- podrska za **Windows Server 2008 R2** i **Windows 7** klijente

WSUS 3.0 SP2 moze se instalirati kao samostalna aplikacija ili nadogradnjom sa verzije 3.0 SP1 pri cemu ostaju sacuvane sve postavke i vec odobrene zakrpe.

Nadogradnjom CARNetovog **WSUS** servisa na verziju 3.0 SP2 omogućeno je i svim ostalim ustanovama koje koriste CARNetov server za skidanje nadogradnji (upstream server) da takodjer pređu na verziju 3.0 SP2 čime mogu koristiti sve nove mogućnosti koje nova verzija donosi.

Više detalja o novoj verziji **WSUS 3.0 SP2** kao i link za preuzimanje možete pronaći na:
http://go.microsoft.com/fwlink/?LinkId=161140 [2]

**WSUS** servis na raspolaganju je preko linka:
http://windowsupdate.carnet.hr:8530/ [3]

Upute o konfiguriranju **WSUS** servera i klijenata nalazi se na stranici:
http://windowsupdate.carnet.hr [4]

**WSUS** instalaciju i odgovarajuću dokumentaciju može se preuzeti sa linka:
http://www.microsoft.com/wsus [5]

U slučaju nejasnoća i problema prilikom instalacije i konfiguracije sustava obratite se na wsus@carnet.hr [6].

sri, 2010-12-15 10:19 - Emil Marmelić**Vijesti:** Windows [7]
**Kategorije:** Sigurnost [8]
**Vote:** 0

No votes yet

**Source URL:** https://sysportal.carnet.hr./node/801

**Links**
[1] http://www.microsoft.com/technet/security/bulletin/ms10-dec.mspx
[2] http://go.microsoft.com/fwlink/?LinkId=161140
[3] http://windowsupdate.carnet.hr:8530/
[4] http://windowsupdate.carnet.hr
[5] http://www.microsoft.com/windowsserversystem/updateservices/downloads/wsus.mspx
[6] mailto:wsus@carnet.hr
[7] https://sysportal.carnet.hr./taxonomy/term/12
[8] https://sysportal.carnet.hr./taxonomy/term/30