



February 2016 Patch Tuesday – All Windows are affected by a critical flaw

February 10, 2016 By [Pierluigi Paganini](#)



Microsoft February 2016 Patch Tuesday updates include a total of 13 bulletins that resolve a total of 41 security flaws in Windows, one of them affects all supported versions.

All supported versions of Windows are affected by a critical vulnerability recently fixed by Microsoft. The IT giant has [released](#) 13 security bulletins, six issues are rated as critical. The security bulletins resolve a total of 41 security flaws in Microsoft software.

One of the bulletins in the February 2016 Patch Tuesday, the MS16-022, fixes the 22 Flash Player flaws recently resolved by Adobe, including the Flash libraries used in Microsoft Internet Explorer 10 and 11, and Edge browsers.

[A vulnerability in the Microsoft Windows 10](#)

security community.

The [MS16-013 vulnerability](#) is a memory-corruption flaw and could be exploited by remote attackers to execute arbitrary code as the logged-in user by tricking a user into opening a specially crafted Journal file. Fortunately, according to Microsoft the vulnerability has not been exploited in the wild.

This vulnerability would allow attackers to run malicious programs on a targeted machine and create new accounts with full user rights.

“The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.” states the official description published by Microsoft.

The list of February 2016 Patch Tuesday bulletins includes also the MS16-015, which fixes critical vulnerabilities in Microsoft Office security that can be exploited to execute arbitrary code in the context of the targeted user simply tricking victims into opening a specially crafted.

The complete list of fixes is reported below:

- MS16-009: A cumulative security update for Internet Explorer 9 through 11. The update patches 13 security issues, including remote-code-execution (RCE) and information disclosure bugs.
- MS16-011: Another cumulative update for the Microsoft’s newest Edge browser in Windows 10 patches 6 security issues, 4 of which are remote code execution vulnerabilities.
- MS16-012: An update addresses two remote-code-execution flaws in Windows PDF Library and Reader for Windows 8.1, Windows 10 and Server 2012. Flaws could allow attackers to run malicious code on an affected system by tricking users into *opening a specially-crafted PDF file*.
- MS16-015: An update patches 6 memory-corruption vulnerabilities in Microsoft Office, each of which could allow a remote attacker to

run arbitrary code by tricking a user into *opening a specially-crafted Office file.*

- MS16-022: A security update resolves more than *two dozen vulnerabilities in Adobe Flash Player* on all supported versions of Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact
MS16-009	Cumulative Security Update for Internet Explorer (1134220) This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution
MS16-011	Cumulative Security Update for Microsoft Edge (1134225) This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Critical Remote Code Execution
MS16-012	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (1133938) This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if Microsoft Windows PDF Library improperly handles application programming interface (API) calls, which could allow an attacker to run arbitrary code on the user's system. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. However, an attacker would have no way to force users to download or open a malicious PDF document.	Critical Remote Code Execution
MS16-013	Security Update for Windows Journal to Address Remote Code Execution (1134811) This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted journal file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical Remote Code Execution

Microsoft also launched a page for public tracking of Windows 10 update ([Windows 10 update history](#)) an effort to show users the improvement applied by the company to its OS.

“We’re committed to our customers and strive to incorporate their feedback, both in how we deliver Windows as a service and the info we provide about Windows 10,” states Microsoft .

“In response to this feedback, we are providing more details about the Windows 10 updates we deliver through Windows Update. You’ll see a summary of important product developments included in each update, with links to more details.”

Pierluigi Paganini

(Security Affairs – Microsoft Windows, Microsoft February 2016 Patch Tuesday)



1. Microsoft Security Patches



SHARE ON



Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS

ARTICLE

**Russian Metel group
manipulated ruble-
dollar exchange rate
with malware**

NEXT ARTICLE

**Crooks are offering
Apple employees
up to \$23,000 for
their login
credentials**

1. Microsoft Security Patches



2. Windows Mobile



3. Windows SDK



4. Microsoft Essentials



5. Windows Security Update



**PROMOTE YOUR
SOLUTIONS ON
SECURITY AFFAIRS
CONTACT US!**



- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".



1. Microsoft Security Patches



2. Windows Mobile



3. Windows SDK



4. Microsoft Essentials



5. Windows Security Update



6. Best Anti Spyware



7. Best Laptop Deals



8. Internet Privacy Protection



Copyright 2015 Security Affairs by Pierluigi Paganini
All Right Reserved.

Back to top ^