



CVE-2017-8461

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-8461
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-15 20:29:00 UTC
Updated	2021-03-29 14:07:00 UTC
Description	Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to e

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Server 2003	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	All	All	All
Operating System	Microsoft	Windows Xp	-	All	All	All
Operating System	Microsoft	Windows Xp	-	All	All	All

References

Reference

- Microsoft Windows RRAS Service MIBEntryGet Overflow ~ Packet Storm
- Microsoft Windows RPC CVE-2017-8461 Remote Code Execution Vulnerability
- Description of the security update of Windows XP and Windows Server 2003: June 13, 2017
- Windows RPC Request Processing Bug in Routing and Remote Access Service Lets Remote Users Execute Arbitrary Code on the Target Sys
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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, advice 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.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)