



CVE-2011-1652

Published on: 04/06/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1652

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 7](#) from [Microsoft](#) contain the following vulnerability:

**** DISPUTED **** The default configuration of Microsoft Windows 7 immediately prefers a new IPv6 and DHCPv6 service over a currently used IPv4 and DHCPv4 service upon receipt of an IPv6 Router Advertisement (RA), and does not provide an option to ignore an unexpected RA, which allows remote attackers to conduct man-in-the-

middle attacks on communication with external IPv4 servers via vectors involving RAs, a DHCPv6 server, and NAT-PT on the local network, aka a "SLAAC Attack." NOTE: it can be argued that preferring IPv6 complies with RFC 3484, and that attempting to determine the legitimacy of an RA is currently outside the scope of recommended behavior of host operating systems.

CVE-2011-1652 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

404 Not Found

Tags

[Exploit](#)

[lists.immunityinc.com](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

Link

[✉ MLIST \[dailydave\] 20110404 SLAAC Attack - Oday Windows Network Interception Configuration Vulnerability](#)

SLAAC Attack – Oday Windows Network Interception Configuration Vulnerability | InfoSec Institute – IT Training and Information Security

[Exploit](#)

[resources.infosecinstitute.com](#)

[I](#) MISC

[resources.infosecinstitute.com/slaac-...](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	All	All	All	All
Operating System	Microsoft	Windows 7	All	All	All	All
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						

Next ID→