



# CVE-2014-4973

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

## Summary

<b>CVE</b>	CVE-2014-4973
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-09-23 15:55:00 UTC
<b>Updated</b>	2014-09-24 14:53:00 UTC
<b>Description</b>	The ESET Personal Firewall NDIS filter (EpFwNdis.sys) driver in the Firewall Module Build 1183 (20140214) and earlier in I

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2113	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2122	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2126	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2214	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2225	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2228	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2113	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2122	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2126	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2214	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2225	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	5.0.2228	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.0.94	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.0.95	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.2.15	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.2.9	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.306	All	All	All

Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.308	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.314	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.316	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.0.94	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.0.95	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.2.15	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	5.2.9	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.306	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.308	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.314	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	6.0.316	All	All	All

## References

Reference	Source	Link	Tags
cve-2014-4973 - Portcullis	MISC	<a href="http://www.portcullis-security.com">www.portcullis-security.com</a>	Exploit
Full Disclosure: CVE-2014-4973 - Privilege Escalation in ESET Windows Products	FULLDISC	<a href="http://seclists.org">seclists.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

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](https://status.cve.report)