CVE-2007-3681

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-3681
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-11 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The IOCTL 9031 (BIOCGSTATS) handler in the NPF.SYS device driver in WinPcap before 4.0.1 allows local users to overv

Risk And Classification

Primary CVSS: v2.0 6.6 from nvd@nist.gov

AV:L/AC:M/Au:S/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Winpcap	Winpcap	3.1	All	All	All

Application	Winpcap	Winpcap	4.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
labs.idefense.com/intelligence/vulnerabilities/display.php	af854a3a-2127-422b-91ae-3
SecurityFocus	af854a3a-2127-422b-91ae-3
SecurityFocus	af854a3a-2127-422b-91ae-3
WinPcap NPF.SYS BIOCGSTATS Parameters Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-3
osvdb.org/37889	af854a3a-2127-422b-91ae-3
SecurityFocus	af854a3a-2127-422b-91ae-3
WinPcap Input Validation Flaw in NPF.SYS Driver Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-3
WinPcap · Change Log	af854a3a-2127-422b-91ae-3
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
WinPcap 4.0 NPF.SYS Privilege Elevation Vulnerability PoC Exploit	af854a3a-2127-422b-91ae-3
WinPcap NPF.SYS IOCTL Handler Privilege Escalation Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-3
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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