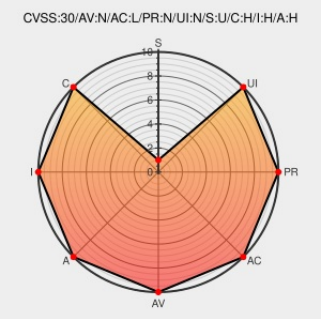
CVE-2018-5701

Published on: 01/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5701

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of System Shield from Iolo contain the following vulnerability:

In Iolo System Shield AntiVirus and AntiSpyware 5.0.0.136, the amp.sys driver file contains an Arbitrary Write vulnerability due to not validating input values from IOCtl 0x00226003.

CVE-2018-5701 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Exploiting System Shield AntiVirus Arbitrary Write Vulnerability using SeTakeOwnershipPrivilege | GreyHatHacker.NET	Exploit, Third Party Advisory, www.greyhathacker.net, text/html	MISC www.greyhathacker.net/?p=1006

System Shield 5.0.0.136 Privilege Escalation ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/146165/System-Shield-5.0.0.136-Privilege-Escalation.html
System Shield 5.0.0.136 - Privilege Escalation - Windows local Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43929

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Iolo	System Shield	5.0.0.136	All	All	All
Application	Iolo	System Shield	5.0.0.136	All	All	All

cpe:2.3:a:iolo:system_shield:5.0.0.136:*:*:*:*:*:*:*

cpe:2.3:a:iolo:system_shield:5.0.0.136:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→