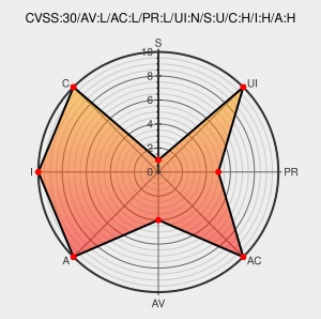
CVE-2018-18435

Published on: 03/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18435

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



Certain versions of Kioware Server from Kioware contain the following vulnerability:

KioWare Server version 4.9.6 and older installs by default to "C:\kioware_com" with weak folder permissions granting any user full permission "Everyone: (F)" to the contents of the directory and it's sub-folders. In addition, the program installs a service called "KWSService" which runs as "Localsystem", this will allow any user to escalate privileges to "NT AUTHORITY\SYSTEM" by substituting the service's binary with a malicious one.

CVE-2018-18435 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
KioWare Server Security Patch Release	Patch	CONFIRM m.kioware.com/news/kioware

KioWare Server Security Patch Release	Patch Vendor Advisory m.kioware.com text/html	CONFIRM m.kioware.com/news/kioware-press-releases/kioware_server_security_patch_update
KioWare Security Patches	Patch Vendor Advisory www.kioware.com text/html	CONFIRM www.kioware.com/patch.aspx
KioWare Server 4.9.6 Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/151031/KioWare-Server-4.9.6-Privilege-Escalation.html
KioWare Server Version 4.9.6 - Weak Folder Permissions Privilege Escalation - Windows local Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 46093
Advisories/ACTIVE-2019-002.md at master · active-labs/Advisories · GitHub	github.com text/html	MISC github.com/active-labs/Advisories/blob/master/2019/ACTIVE-2019-002.md

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kioware	Kioware Server	All	All	All	All

cpe:2.3:a:kioware:kioware_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→