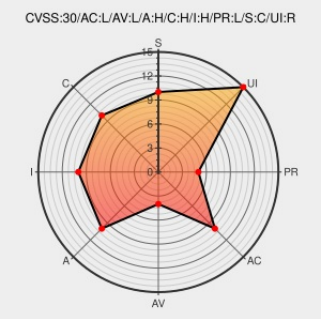
CVE-2020-13386

Published on: 05/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-13386

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



Certain versions of Smartdraw 2020 from Smartdraw contain the following vulnerability:

In SmartDraw 2020 27.0.0.0, the installer gives inherited write permissions to the Authenticated Users group on the SmartDraw 2020 installation folder. Additionally, when the product is installed, two scheduled tasks are created on the machine, SDMsgUpdate (Local) and SDMsgUpdate (TE). The scheduled tasks run in the context of the user who installed the product. Both scheduled tasks attempt to run the same binary, C:\SmartDraw 2020\Messages\SDNotify.exe. The folder Messages doesn't exist by default and (by extension) neither does SDNotify.exe. Due to the weak folder permissions, these can be created by any user. A malicious actor can therefore create a malicious SDNotify.exe binary, and have it automatically run, whenever the user who installed the product logs on to the machine. The malicious SDNotify.exe could, for example, create a new local administrator account on the machine.

CVE-2020-13386 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Weak folder permissions potentially leading to privilege escalation in SmartDraw 2020 — Improsec | improving security	Exploit Third Party Advisory improsec.com text/html	MISC improsec.com/tech-blog/how-not-do-handle-responsible-disclosure-smartdraw-2020

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Smartdraw	Smartdraw 2020	27.0.0.0	All	All	All
Application	Smartdraw	Smartdraw 2020	27.0.0.0	All	All	All

cpe:2.3:a:smartdraw:smartdraw_2020:27.0.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:smartdraw:smartdraw_2020:27.0.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→