

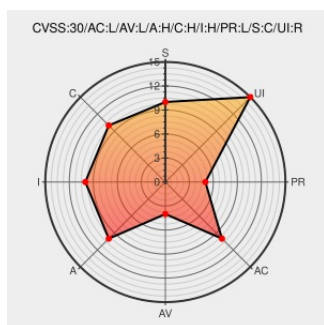


CVE-2020-13386

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 [M](#) 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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
<code>cpe:2.3:a:smartdraw:smartdraw_2020:27.0.0.0:*:*:*:*:*:</code>						
<code>cpe:2.3:a:smartdraw:smartdraw_2020:27.0.0.0:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023   |

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](#)