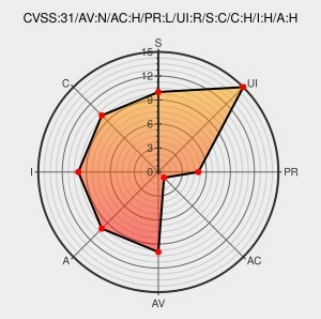
CVE-2020-15264

Published on: 10/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15264 - advisory for GHSA-rpgx-h675-r3jf

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



Certain versions of Boxstarter from Chocolatey contain the following vulnerability:

The Boxstarter installer before version 2.13.0 configures C:\ProgramData\Boxstarter to be in the system-wide PATH environment variable. However, this directory is writable by normal, unprivileged users. To exploit the vulnerability, place a DLL in this directory that a privileged service is looking for. For example, WptsExtensions.dll When Windows starts, it'll execute the code in DllMain() with SYSTEM privileges. Any unprivileged user can execute code with SYSTEM privileges. The issue is fixed in version 3.13.0

CVE-2020-15264 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **chocolatey** - **boxstarter** version **< 2.13.0**

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-rpgx-h675-r3jf · chocolatey/boxstarter@67e3204 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/chocolatey/boxstarter/commit/67e320491813550b48900e87105a34ceefc
VU#208577 - Chocolatey Boxstarter vulnerable to privilege escalation due to weak ACLs	Third Party Advisory www.kb.cert.org text/html	CERT-VN VU#208577
Boxstarter folder allows write access for standard users · Advisory · chocolatey/boxstarter · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/chocolatey/boxstarter/security/advisories/GHSA-rpgx-h675

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chocolatey	Boxstarter	All	All	All	All
Application	Chocolatey	Boxstarter	All	All	All	All

cpe:2.3:a:chocolatey:boxstarter:*:*:*:*:*:*:*:*:

cpe:2.3:a:chocolatey:boxstarter:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→