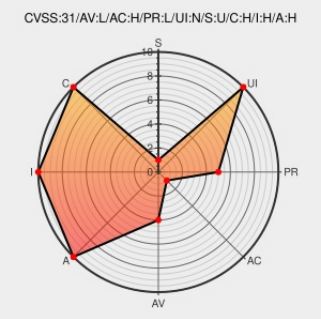
CVE-2022-26488

Published on: Not Yet Published

Last Modified on: 09/03/2022 03:34:00 AM UTC

CVE-2022-26488

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



Certain versions of Windows from Microsoft contain the following vulnerability:

In Python before 3.10.3 on Windows, local users can gain privileges because the search path is inadequately secured. The installer may allow a local attacker to add user-writable directories to the system search path. To exploit, an administrator must have installed Python for all users and enabled PATH entries. A non-administrative user can trigger a repair that incorrectly adds user-writable paths into PATH, enabling search-path hijacking of other users and system services. This affects Python (CPython) through 3.7.12, 3.8.x through 3.8.12, 3.9.x through 3.9.10, and 3.10.x through 3.10.2.

CVE-2022-26488 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
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

Mailman 3 [CVE-2022-26488] Escalation of privilege via Windows installer - Security-announce - python.org	mail.python.org text/html	MISC mail.python.org/archives/list/security-announce@python.org/thread/657Z4XULWZNIY5FRP3OWXHYKUSIH6DMN/
CVE-2022-26488 Python Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220419-0005/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Python	Python	3.11.0	alpha1	All	All
Application	Python	Python	3.11.0	alpha2	All	All
Application	Python	Python	3.11.0	alpha3	All	All
Application	Python	Python	3.11.0	alpha4	All	All
Application	Python	Python	3.11.0	alpha5	All	All
Application	Python	Python	3.11.0	alpha6	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*:

cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha3:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha4:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha5:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.11.0:alpha6:*:*:*:*:*:*:

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@zooba	CVE-2022-26488 is now published. Email announcement linked below. Short version, if you installed Python as admin… twitter.com/i/web/status/1…	2022-03-07 16:57:17
@CVEreport	CVE-2022-26488 : In Python before 3.10.3 on #Windows, local users can gain privileges because the search path is in… twitter.com/i/web/status/1…	2022-03-10 17:45:15

← Previous ID

Next ID→