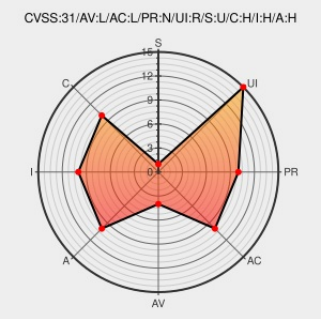
CVE-2020-4588

Published on: 10/30/2020 12:00:00 AM UTC

Last Modified on: 09/30/2022 11:16:00 PM UTC

CVE-2020-4588

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



Certain versions of I2 Ibase from Ibm contain the following vulnerability:

IBM i2 iBase 8.9.13 could allow an attacker to upload arbitrary executable files which, when executed by an unsuspecting victim could result in code execution. IBM X-Force ID: 184579.

CVE-2020-4588 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **IBM** - **i2 iBase** version **8.9.13**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin: iBase unrestricted file upload	Patch, Vendor Advisory, www.ibm.com	CONFIRM www.ibm.com/support/pages/node/6357037

	text/html	
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-i2-cve20204588-file-upload (184579)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	I2 Ibase	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:ibm:i2_ibase:*:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | IBM i2 iBase 8.9.13 could allow an attac... | CVE-2020-4588 | Link for more: alerts.remotelyrmm.com/CVE-2020-4588	2022-10-01 00:29:50

← Previous ID

Next ID→