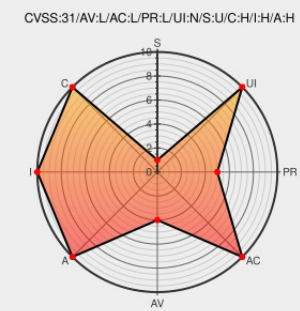
CVE-2021-29665

Published on: 05/31/2021 12:00:00 AM UTC

Last Modified on: 06/07/2021 07:37:00 PM UTC

CVE-2021-29665

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



Certain versions of Security Verify Access from Ibm contain the following vulnerability:

IBM Security Verify Access 20.07 is vulnerable to a stack based buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with elevated privileges.

CVE-2021-29665 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **IBM** - **Security Verify Access** version **20.07**

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: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin: Multiple Security Vulnerabilities have been resolved in IBM Application Gateway (CVE-2021-20576, CVE-2021-20575, CVE-2021-29665)	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6457315

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-ag-cve202129665-bo (199399)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Security Verify Access	20.07	All	All	All

cpe:2.3:a:ibm:security_verify_access:20.07:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29665 : #IBM Security Verify Access 20.07 is vulnerable to a stack based buffer overflow, caused by improp… twitter.com/i/web/status/1…	2021-05-31 15:45:05
/r/netcve	CVE-2021-29665	2021-05-31 16:41:31

← Previous ID

Next ID→