

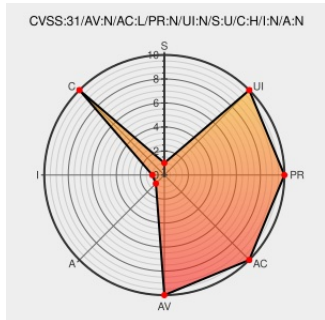


# CVE-2020-4400

Published on: 07/22/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

## CVE-2020-4400

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Verify Gateway](#) from [Ibm](#) contain the following vulnerability:

IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 179478.

CVE-2020-4400 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **Verify Gateway (IVG)** version **1.0.0**

Affected Vendor/Software: [IBM](#) - **Verify Gateway (IVG)** version **1.0.1**

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description            | Tags                          | Link                          |
|------------------------|-------------------------------|-------------------------------|
| IBM X-Force ID: 179478 | <a href="#">CVE-2020-4400</a> | <a href="#">CVE-2020-4400</a> |

IBM X-Force Exchange

VDB Entry

Vendor Advisory

exchange.xforce.ibmcloud.com

text/html

XF

ibm-ivg-cve20204400-info-disc

(179478)

Security Bulletin: IBM Verify Gateway does not prevent excessive authentication attempts (CVE-2020-4400)

Patch

Vendor Advisory

www.ibm.com

text/html

CONFIRM

www.ibm.com/support/pages/node/6251279

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](mailto: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 | ibm    | Verify Gateway | 1.0.0   | All    | All     | All      |
| Application | ibm    | Verify Gateway | 1.0.1   | All    | All     | All      |
| Application | ibm    | Verify Gateway | 1.0.0   | All    | All     | All      |
| Application | ibm    | Verify Gateway | 1.0.1   | All    | All     | All      |

cpe:2.3:a:ibm:verify\_gateway:1.0.0:\*\*\*\*:\*\*\*\*:

cpe:2.3:a:ibm:verify\_gateway:1.0.1:\*\*\*\*:\*\*\*\*:

cpe:2.3:a:ibm:verify\_gateway:1.0.0:\*\*\*\*:\*\*\*\*:

cpe:2.3:a:ibm:verify\_gateway:1.0.1:\*\*\*\*:\*\*\*\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →