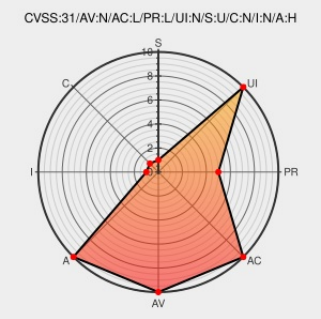
# CVE-2020-4485

Published on: 08/11/2020 12:00:00 AM UTC

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

## CVE-2020-4485

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




Certain versions of Qradar Security Information And Event Manager from Ibm contain the following vulnerability:

IBM QRadar 7.2.0 through 7.2.9 could allow an authenticated user to disable the Wincollect service which could aid an attacker in bypassing security mechanisms in future attacks. IBM X-Force ID: 181860.

CVE-2020-4485 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **IBM** - **QRadar Wincollect** version **7.2.0**

Affected Vendor/Software: **IBM** - **QRadar Wincollect** version **7.2.9**

### CVSS3 Score: 6.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 4 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| Security Bulletin: IBM QRadar Wincollect is vulnerable to improper access control (CVE-2020-4485, CVE-2020-4486) | Vendor Advisory<br>www.ibm.com<br>text/html | CONFIRM<br>www.ibm.com/support/pages/node/6257885 |
| IBM X-Force Exchange | VDB Entry<br>Vendor Advisory<br>exchange.xforce.ibmcloud.com<br>text/html | XF ibm-qradar-cve20204485-dos (181860) |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Ibm | Qradar Security Information And Event Manager | All | All | All | All |

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→