

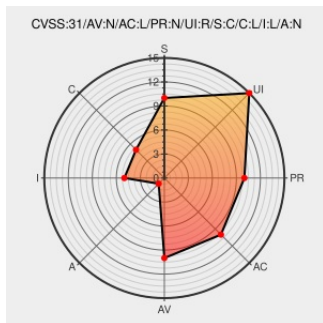


# CVE-2019-19368

Published on: 12/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:53 PM UTC

## CVE-2019-19368

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

Certain versions of [Rumpus](#) from [Maxum](#) contain the following vulnerability:

A Reflected Cross Site Scripting was discovered in the Login page of Rumpus FTP Web File Manager 8.2.9.1. An attacker can exploit it by sending a crafted link to end users and can execute arbitrary Javascripts

CVE-2019-19368 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

## CVE References

| Description                                   | Tags                                                                                          | Link                                                           |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Download   Rumpus                             | <a href="#">Vendor Advisory</a><br><a href="#">www.maxum.com</a><br><a href="#">text/html</a> | <a href="#">MISC www.maxum.com/Rumpus/Download.html</a>        |
| GitHub - harshit-shukla/CVE: CVE's for Rumpus | <a href="#">Exploit</a>                                                                       | <a href="#">MISC github.com/harshit-shukla/CVE-2019-19368/</a> |

FTP Server

Third Party Advisory

github.com

text/html

Rumpus FTP Web File Manager 8.2.9.1 Cross Site Scripting ≈ Packet Storm

Exploit

Third Party Advisory

packetstormsecurity.com

text/html

📄

MISC packetstormsecurity.com/files/155719/Rumpus-FTP-Web-File-Manager-8.2.9.1-Cross-Site-Scripting.html

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 | Maxum  | Rumpus  | 8.2.9.1 | All    | All     | All      |
| Application | Maxum  | Rumpus  | 8.2.9.1 | All    | All     | All      |

cpe:2.3:a:maxum:rumpus:8.2.9.1:\*\*\*\*\*:

cpe:2.3:a:maxum:rumpus:8.2.9.1:\*\*\*\*\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→