



# CVE-2018-19586

Published on: 04/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

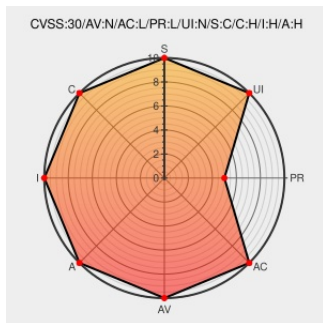
## CVE-2018-19586

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Silverpeas 5.15 through 6.0.2 is affected by an authenticated Directory Traversal vulnerability that can be triggered during file uploads because core/webapi/upload/FileUploadData.java mishandles a StringUtil.java call. This vulnerability enables regular users to write arbitrary files on the underlying system with privileges of the user

running the application. Especially, an attacker may leverage the vulnerability to write an executable JSP file in an exposed web directory to execute commands on the underlying system.

CVE-2018-19586 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.9 - CRITICAL**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>COMPLETE</b>	<b>COMPLETE</b>	<b>COMPLETE</b>

## CVE References

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

Silverpeas 5.15 To 6.0.2: Path Traversal - Bishop Fox

Exploit  
Third Party Advisory  
www.bishopfox.com  
text/html

MISC [www.bishopfox.com/news/2019/01/silverpeas-5-15-to-6-0-2-path-traversal/](http://www.bishopfox.com/news/2019/01/silverpeas-5-15-to-6-0-2-path-traversal/)

Silverpeas-Core/FileUploadData.java at d8c3bbb0695a4907db013401bd16c6527e2b4f41 · Silverpeas/Silverpeas-Core · GitHub

Patch  
Third Party Advisory  
github.com  
text/html

MISC [github.com/Silverpeas/Silverpeas-Core/blob/d8c3bbb0695a4907db013401bd16c6527e2b4f41/core-web/src/main/java/org/silverpeas/core/webapi/upload/FileUploadData.java](https://github.com/Silverpeas/Silverpeas-Core/blob/d8c3bbb0695a4907db013401bd16c6527e2b4f41/core-web/src/main/java/org/silverpeas/core/webapi/upload/FileUploadData.java)

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	<a href="#">Silverpeas</a>	<a href="#">Silverpeas</a>	All	All	All	All
<code>cpe:2.3:a:silverpeas:silverpeas:*:*:*:*:*:*</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**