



## IPS Intrusion Prevention

# Seeyon.Office.Anywhere.htmlofficeservlet.Arbitrary.File.Upload



ID	48874
Created	Apr 13, 2020
Updated	Apr 16, 2020
Risk	<span style="color: green;">●</span> <span style="color: green;">●</span> <span style="color: green;">●</span> <span style="color: green;">●</span> <span style="color: gray;">●</span>
Default Action	drop
Active	<input checked="" type="checkbox"/>
Affected OS	Other
Affected App	Other
Profile Type	OS Command Injection

### Description

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

Accept

Seeyon A8-V5 Collaborative Management Software V6. 1sp1

Seeyon A8+ Collaborative Management Software V7. 0, V7. 0sp1, V7. 0sp2, V7. 0sp3


Seeyon A8+ Collaborative Management Software V7. 1

## Impact

System Compromise: Remote attackers can gain control of vulnerable systems.

## Recommended Actions

Currently we are not aware any vendor provided patch to address this issue.

Loading ... 

## Coverage

IPS (Regular DB)



IPS (Extended DB)



## Version Updates

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

<https://www.lsablog.com/networksec/penetration/seeyon-oa-file-upload-vulnerability-analysis/>

**FORTINET**®

[Contact Us](#) | [Legal](#) | [Privacy](#) | [Partners](#) | [Feedback](#)



Copyright © 2026 Fortinet, Inc. All Rights Reserved.

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).