Contents

Security:Security Advisories

Release name	Release date	Title	References	Summary
BSSA-2023-01	2023-07-25	Ghostscript vulnerability	CVE-2023-36664	Code can be executed on the server via a manipulated PDF
BSSA-2022-08	2022-11-15	XSS attack vector on regular pages	CVE-2022-3895	Arbitrary HTML injection through use of interface elements
BSSA-2022-07	2022-11-15	XSS attack vector on regular pages	CVE-2022-3958	Arbitrary HTML injection through personal menu items
BSSA-2022-06	2022-11-15	XSS attack vector on regular pages	CVE-2022-3893	Arbitrary HTML injection through the custom menu
BSSA-2022-05	2022-11-15	XSS attack vector on regular pages	CVE-2022-42001	Arbitrary HTML injection through the book navigation
BSSA-2022-04	2022-11-15	XSS attack vector on regular pages	CVE-2022-41789, CVE-2022-41814, CVE-2022-42000	Arbitrary HTML injection through user preferences
BSSA-2022-03	2022-11-15	XSS attack vector on regular pages	CVE-2022-41611	Arbitrary HTML injection through main navigation
BSSA-2022-02	2022-11-15	XSS attack vector on regular pages	CVE-2022-2511	Arbitrary HTML injection through the 'title' parameter
BSSA-2022-01	2022-01-31	XSS attack vector in Search Center	CVE-2022-2510	JavaScript in search field is reflected back to the browser.

Security:Security Advisories/BSSA-2022-01

Date	2022-01-31
Severity	Medium
Affected	BlueSpice 3.x, BlueSpice 4.x
	BlueSpice 3.2.9, BlueSpice

Fixed in	4.1.1
CVE	CVE-2022-2510

Problem

Users are able to inject arbitrary HTML (XSS) on Special:SearchCenter, using the search term. This can be triggered via URL.

Solution

Upgrade to BlueSpice 4.1.1

Acknowledgements

Special thanks to the security team of an undisclosed customer

Security:Security Advisories/BSSA-2022-02

Date	2022-04-25
Severity	Medium
Affected	BlueSpice 4.x
Fixed in	4.1.3
CVE	CVE-2022-2511

Problem

Users are able to inject arbitrary HTML (XSS) on regular pages, using a special value for the `title` parameter. This can be triggered via URL.

Solution

Upgrade to BlueSpice 4.1.3

Acknowledgements

Special thanks to the security team of an undisclosed customer

Security:Security Advisories/BSSA-2022-03

Date	2022-11-15
Severity	Low
Affected	BlueSpice 4.x
Fixed in	BlueSpice 4.2.1
CVE	CVE-2022-41611

Problem

Users with admin rights are able to inject arbitrary HTML (XSS) into main navigation by editing a menu item.

Solution

Upgrade to BlueSpice 4.2.1

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2022-04

Date	2022-11-15
Severity	Low
Affected	BlueSpice 4.x
Fixed in	BlueSpice 4.2.1
CVE	• CVE-2022-41789 • CVE-2022-41814 • CVE-2022-42000

Problem

Logged in users are able to inject arbitrary HTML (XSS) into several locations in the main interface by editing their user preferences.

Solution

Upgrade to BlueSpice 4.2.1

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2022-05

Date	2022-11-15
Severity	Low
Affected	BlueSpice 4.x
Fixed in	BlueSpice 4.2.1
CVE	CVE-2022-42001

Problem

Users with edit rights are able to inject arbitrary HTML (XSS) into book navigation by editing a book chapter title.

Solution

Upgrade to BlueSpice 4.2.1

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2022-06

Date	2022-11-15
Severity	Low
Affected	BlueSpice 4.x
Fixed in	BlueSpice 4.2.1
CVE	CVE-2022-3893

Problem

Users with admin rights are able to inject arbitrary HTML (XSS) into custom navigation by editing a menu item.

Solution

Upgrade to BlueSpice 4.2.1

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2022-07

Date	2022-11-15
Severity	Medium
Affected	BlueSpice 4.x
Fixed in	BlueSpice 4.2.1
CVE	CVE-2022-3958

Problem

Users with edit rights are able to inject arbitrary HTML (XSS) into a user's personal navigation by editing a menu item. This allows for targeted attacks

Solution

Upgrade to BlueSpice 4.2.1

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2022-08

Date	2022-11-15
Severity	Medium
Affected	• BlueSpice 4.x • Common User Interface 3.0.x
Fixed in	• BlueSpice 4.2.1 • Common User Interface 3.0.5
CVE	CVE-2022-3895

Problem

Some UI elements of the Common user interface component are not properly sanitizing output and therefore prone to output arbitrary HTML (XSS).

Solution

Upgrade to Common User Interface 3.0.5 or later. This is included in BlueSpice 4.2.1 or later.

Acknowledgements

Found during an internal security audit.

Security:Security Advisories/BSSA-2023-01

Date	2023-07-25
Severity	Medium

Affected	• BlueSpice Infrastructure: Ghostscript
Fixed in	• Ghostscript 9.53.3 and 10.01.2
CVE	CVE-2023-36664

Contents

Problem

A bug in ghostscript can be exploited to run arbitrary code on the host machine using prepared PDF document. In BlueSpice, when a) PDFHandler is enabled and b) a PDF document is uploaded, a preview image is being generated using ghostscript. If an attacker uploads a prepared PDF, they can execute code on the server.

PDFHandler is not enabled by default, but many installations have set it active.

Solution

Upgrade Ghostscript to a fixed version and ensure the updated version is used by adding `$wgPdfProcessor = '/usr/bin/gs';` to `LocalSettings.php`.

If upgrade of Ghostscript is not possible, disable the extension PDFHandler. This, however, removes the ability for BlueSpice to render PDF preview images.

Resources

- For Debian: https://www.debian.org/security/2023/dsa-5446
- For Debian10: Information on source package ghostscript (debian.org)
- For Ubuntu: https://launchpad.net/ubuntu/+source/ghostscript/9.50~dfsg-5ubuntu4.8

Acknowledgements

Found during an internal security audit.