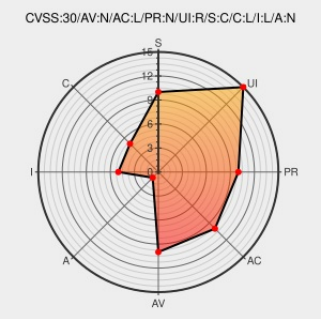
CVE-2015-7360

Published on: 05/26/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7360

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



Certain versions of Fortisandbox from Fortinet contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the Web User Interface (WebUI) in Fortinet FortiSandbox before 2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) serial parameter to alerts/summary/profile/; the (2) urlForCreatingReport parameter to csearch/report/export/; the (3) id parameter to analysis/detail/download/screenshot; or vectors related to (4) "Fortiview threats by users search filtered by vdom" or (5) "PCAP file download generated by the VM scan feature."

CVE-2015-7360 has been assigned by 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
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link

	hyp3rlinx.altervista.org text/plain	MISC hyp3rlinx.altervista.org/advisories/AS-FORTISANDBOX-0801.txt
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20150801 Multiple XSS vulnerabilities in FortiSandbox WebUI
FortiSandbox 3000D 2.02 build0042 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/132930/FortiSandbox-3000D-2.02-build0042-Cross-Site-Scripting.html
FortiGuard	Vendor Advisory fortiguard.com text/html Inactive Link Not Archived	CONFIRM fortiguard.com/advisory/multiple-xss-vulnerabilities-in-fortisandbox-webui

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Fortinet	Fortisandbox	-	All	All	All
Hardware	Fortinet	Fortisandbox	-	All	All	All
Operating System	Fortinet	Fortisandbox Firmware	All	All	All	All

cpe:2.3:h:fortinet:fortisandbox:-:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:fortisandbox:-:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortisandbox_firmware:*:*:*:*:*:*:*:*:

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 registred 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