



CVE-2017-8440

Published on: 06/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

CVE-2017-8440

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Starting in version 5.3.0, Kibana had a cross-site scripting (XSS) vulnerability in the Discover page that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users.

CVE-2017-8440 has been assigned by security@elastic.co to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Elastic - Kibana** version **5.3.0 to 5.3.3**

Affected Vendor/Software: **Elastic - Kibana** version **5.4.1**

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
CVSS: 5.4.1 - 5.9.3 - 5.9.3 - 5.9.3 - 5.9.3 - 5.9.3 - 5.9.3 - 5.9.3	CONFIRM	CONFIRM

Kibana 5.4.1 and 5.3.3 released Elastic Blog	Release Notes Vendor Advisory www.elastic.co text/html	 CONFIRM www.elastic.co/blog/kibana-5-4-1-and-5-3-3-released
Elastic Stack 5.4.1 and 5.3.3 Security updates - Security Announcements - Discuss the Elastic Stack	Mitigation Vendor Advisory discuss.elastic.co text/html	 CONFIRM discuss.elastic.co/t/elastic-stack-5-4-1-and-5-3-3-security-updates/87952
Security issues Elastic	Vendor Advisory www.elastic.co text/html	 CONFIRM www.elastic.co/community/security

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
Application	Elastic	Kibana	5.3.0	All	All	All
Application	Elastic	Kibana	5.3.1	All	All	All
Application	Elastic	Kibana	5.3.2	All	All	All
Application	Elastic	Kibana	5.4.0	All	All	All
Application	Elastic	Kibana	5.3.0	All	All	All
Application	Elastic	Kibana	5.3.1	All	All	All
Application	Elastic	Kibana	5.3.2	All	All	All
Application	Elastic	Kibana	5.4.0	All	All	All
cpe:2.3:a:elastic:kibana:5.3.0:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.3.1:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.3.2:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.4.0:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.3.0:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.3.1:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.3.2:*:*:*:*:*:						
cpe:2.3:a:elastic:kibana:5.4.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#)