



CVE-2019-12668

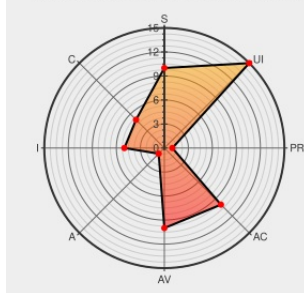
Published on: 09/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-12668 - advisory for cisco-sa-20190925-sbxss

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N



Certain versions of **ios** from **Cisco** contain the following vulnerability:

A vulnerability in the web framework code of Cisco IOS and Cisco IOS XE Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected software using the banner parameter. The vulnerability is due to insufficient input validation of the banner parameters that are passed to the web server of the affected software.

An attacker could exploit this vulnerability by crafting a banner parameter and saving it. The attacker could then convince a user of the web interface to access a malicious link or could intercept a user request for the affected web interface and inject malicious code into the request. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information.

CVE-2019-12668 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco IOS XE Software 3.6.0E** version n/a

CVSS3 Score: **4.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco IOS and IOS XE Software Stored Banner Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190925 Cisco IOS and IOS XE Software Stored Banner Cross-Site Scripting Vulnerability

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
Operating System	Cisco	ios	15.2(2)e	All	All	All
Operating System	Cisco	ios	15.2(2)ea	All	All	All
Operating System	Cisco	ios	15.2(3)e	All	All	All
Operating System	Cisco	ios	15.2(3)ea	All	All	All
Operating System	Cisco	ios	15.2(4)e	All	All	All
Operating System	Cisco	ios	15.2(4)ea	All	All	All
Operating System	Cisco	ios	15.2(4)ec	All	All	All
Operating System	Cisco	ios	15.2(5)e	All	All	All
Operating System	Cisco	ios	15.2(5)ea	All	All	All
Operating System	Cisco	ios	15.2(5)ex	All	All	All
Operating System	Cisco	ios	15.2(6)e	All	All	All
Operating System	Cisco	ios	15.2(7)e	All	All	All
Operating System	Cisco	ios	15.2\2\)	All	All	All

Operating System	Cisco	ios	15.2\2\ea	All	All	All
Operating System	Cisco	ios	15.2\3\ea	All	All	All
Operating System	Cisco	ios	15.2\3\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ec	All	All	All
Operating System	Cisco	ios	15.2\5\ea	All	All	All
Operating System	Cisco	ios	15.2\5\ea	All	All	All
Operating System	Cisco	ios	15.2\5\ex	All	All	All
Operating System	Cisco	ios	15.2\6\ea	All	All	All
Operating System	Cisco	ios	15.2\7\ea	All	All	All
Operating System	Cisco	ios	15.2\2\ea	All	All	All
Operating System	Cisco	ios	15.2\2\ea	All	All	All
Operating System	Cisco	ios	15.2\3\ea	All	All	All
Operating System	Cisco	ios	15.2\3\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ea	All	All	All
Operating System	Cisco	ios	15.2\4\ec	All	All	All
Operating System	Cisco	ios	15.2\5\ea	All	All	All
Operating System	Cisco	ios	15.2\5\ea	All	All	All
Operating System	Cisco	ios	15.2\5\ex	All	All	All
Operating System	Cisco	ios	15.2\6\ea	All	All	All
Operating System	Cisco	ios	15.2\7\ea	All	All	All

Operating System	Cisco	ios Xe	All	All	All	All
Operating System	Cisco	ios Xe	16.1.1	All	All	All
Operating System	Cisco	ios Xe	3.10e	All	All	All
Operating System	Cisco	ios Xe	3.6e	All	All	All
Operating System	Cisco	ios Xe	3.7e	All	All	All
Operating System	Cisco	ios Xe	3.8e	All	All	All
Operating System	Cisco	ios Xe	3.9e	All	All	All
Operating System	Cisco	ios Xe	All	All	All	All
Operating System	Cisco	ios Xe	3.10e	All	All	All
Operating System	Cisco	ios Xe	3.6e	All	All	All
Operating System	Cisco	ios Xe	3.7e	All	All	All
Operating System	Cisco	ios Xe	3.8e	All	All	All
Operating System	Cisco	ios Xe	3.9e	All	All	All
cpe:2.3:o:cisco:ios:15.2(2)e:*****:						
cpe:2.3:o:cisco:ios:15.2(2)ea:*****:						
cpe:2.3:o:cisco:ios:15.2(3)e:*****:						
cpe:2.3:o:cisco:ios:15.2(3)ea:*****:						
cpe:2.3:o:cisco:ios:15.2(4)e:*****:						
cpe:2.3:o:cisco:ios:15.2(4)ea:*****:						
cpe:2.3:o:cisco:ios:15.2(4)ec:*****:						
cpe:2.3:o:cisco:ios:15.2(5)e:*****:						
cpe:2.3:o:cisco:ios:15.2(5)ea:*****:						
cpe:2.3:o:cisco:ios:15.2(5)ex:*****:						
cpe:2.3:o:cisco:ios:15.2(6)e:*****:						
cpe:2.3:o:cisco:ios:15.2(7)e:*****:						

```
cpe:2.3:o:cisco:ios:15.2(2)e:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.2\2\ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2\((3\)e:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.2(3)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)ec:~::~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(5)e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(5)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(5)ex:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2\ (6\ )e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(7)e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(2)e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(2)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2\ (3) e:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.2(3)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(4)ec:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2\5:e:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.2(5)ea:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2(5)ex:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.2\ (6\ )e:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.2\ (7\ )e:~::~::~:
```

```
cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios_xe:16.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios_xe:3.10e:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios_xe:3.6e:*.:.:.:.:.:
```

cpe:2.3:o:cisco:ios_xe:3.7e:*****:
cpe:2.3:o:cisco:ios_xe:3.8e:*****:
cpe:2.3:o:cisco:ios_xe:3.9e:*****:
cpe:2.3:o:cisco:ios_xe:*****:
cpe:2.3:o:cisco:ios_xe:3.10e:*****:
cpe:2.3:o:cisco:ios_xe:3.6e:*****:
cpe:2.3:o:cisco:ios_xe:3.7e:*****:
cpe:2.3:o:cisco:ios_xe:3.8e:*****:
cpe:2.3:o:cisco:ios_xe:3.9e:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)