



CVE-2021-34759

Published on: 09/01/2021 12:00:00 AM UTC

Last Modified on: 09/10/2021 05:28:00 PM UTC

CVE-2021-34759 - advisory for cisco-sa-ise-xss-4HnZFewr

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Identity Services Engine** from **Cisco** contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not

properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need valid administrative credentials.

CVE-2021-34759 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 aware that proof-of-concept exploit code is available for the vulnerability described in this advisory.

Affected Vendor/Software: **Cisco - Cisco Identity Services Engine Software** 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 Identity Services Engine Cross-Site Scripting Vulnerability	tools.cisco.com text/html	CISCO 20210901 Cisco Identity Services Engine 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.		

Related QID Numbers

317026 Cisco Identity Services Engine (ISE) Cross-Site Scripting (XSS) Vulnerability (cisco-sa-ise-xss-4HnZFewr)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	All	All	All	All
Application	Cisco	Identity Services Engine	2.2.0	-	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch1	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch10	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch12	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch13	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch14	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch15	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch16	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch17	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch2	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch3	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch4	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch5	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch6	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch7	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch8	All	All
Application	Cisco	Identity Services Engine	2.2.0	patch9	All	All
Application	Cisco	Identity Services Engine	2.3.0	-	All	All
Application	Cisco	Identity Services Engine	2.3.0	patch1	All	All

Application	Cisco	Identity Services Engine	3.0.0	patch2	All	All
Application	Cisco	Identity Services Engine	3.0.0	patch3	All	All
cpe:2.3:a:cisco:identity_services_engine:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:-*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch1:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch10:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch12:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch13:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch14:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch15:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch16:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch17:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch2:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch3:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch4:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch5:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch6:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch7:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch8:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.2.0:patch9:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:-*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch1:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch2:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch3:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch4:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch5:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch6:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.3.0:patch7:*.***.***.*:						
cpe:2.3:a:cisco:identity_services_engine:2.4.0:-*.***.***.*:						

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch1:*.:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch10:::*.*.*.*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch11:*.:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch12:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch13:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch14:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch2:*.:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch3:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch4:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch5:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch6:::*:*:*::
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch7:*.:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch8:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0:patch9:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:-:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch1:::*:*:*::
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch2:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch3:*.:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch5:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch6:::*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch7:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch8:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch9:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch1:::*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch2:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch3:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch4:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:3.0.0:patch1:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:3.0.0:batch2:*:*:*:*.*
```

cpe:2.3:a:cisco:identity_services_engine:3.0.0:patch3:****:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @management_sun	IT Risk:Cisco.Identity Services Engine (ISE)に脆弱性 CVE-2021-34759 tools.cisco.com/security/cente... auscert.org.au/bulletins/ESB-...	2021-09-01 23:53:29
 @CVEreport	CVE-2021-34759 : A vulnerability in the web-based management interface of Cisco Identity Services Engine ISE So... twitter.com/i/web/status/1...	2021-09-02 03:15:21
 @softek_jp	Cisco ISE Software の Web 管理インターフェイスの処理にクロスサイトスクリプティングの問題 (CVE-2021-34759) [39873] sid.softek.jp/content/show/3... #SIDfm #脆弱性情報	2021-09-02 07:43:12
 @threatmeter	CVE-2021-34759 A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Softwa... twitter.com/i/web/status/1...	2021-09-03 07:09:53

← 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 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](#)