



CVE-2019-12638

Published on: 10/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12638 - advisory for cisco-sa-20191016-ise-store-xss

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) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input that is processed by the

web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.

CVE-2019-12638 has been assigned by [Cisco PSIRT](#) 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 Identity Services Engine Software** version n/a

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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	Integrity	Availability

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20191016 Cisco Identity Services Engine Stored 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
Application	Cisco	Identity Services Engine	2.3	-	All	All
Application	Cisco	Identity Services Engine	2.3	patch1	All	All
Application	Cisco	Identity Services Engine	2.3	patch2	All	All
Application	Cisco	Identity Services Engine	2.3	patch3	All	All
Application	Cisco	Identity Services Engine	2.3	patch5	All	All
Application	Cisco	Identity Services Engine	2.3	patch6	All	All
Application	Cisco	Identity Services Engine	2.3	patch7	All	All
Application	Cisco	Identity Services Engine	2.3(0.298)	All	All	All
Application	Cisco	Identity Services Engine	2.3\0.298\	All	All	All
Application	Cisco	Identity Services Engine	2.4	-	All	All
Application	Cisco	Identity Services Engine	2.4	patch1	All	All
Application	Cisco	Identity Services Engine	2.4	patch2	All	All
Application	Cisco	Identity Services Engine	2.4	patch3	All	All
Application	Cisco	Identity Services Engine	2.4	patch5	All	All
Application	Cisco	Identity Services Engine	2.4	patch6	All	All
Application	Cisco	Identity Services Engine	2.4	patch7	All	All
Application	Cisco	Identity Services Engine	2.4	patch8	All	All
Application	Cisco	Identity Services Engine	2.4	patch9	All	All
Application	Cisco	Identity Services Engine	2.4(0.357)	All	All	All
Application	Cisco	Identity Services Engine	2.4\0.357\	All	All	All
Application	Cisco	Identity Services Engine	2.6(0.156)	All	All	All

Application	Cisco	Identity Services Engine	2.6\0.156\)	All	All	All
Application	Cisco	Identity Services Engine	2.7(0.999)	All	All	All
Application	Cisco	Identity Services Engine	2.7\0.999\)	All	All	All
Application	Cisco	Identity Services Engine	2.3	-	All	All
Application	Cisco	Identity Services Engine	2.3	patch1	All	All
Application	Cisco	Identity Services Engine	2.3	patch2	All	All
Application	Cisco	Identity Services Engine	2.3	patch3	All	All
Application	Cisco	Identity Services Engine	2.3	patch5	All	All
Application	Cisco	Identity Services Engine	2.3	patch6	All	All
Application	Cisco	Identity Services Engine	2.3	patch7	All	All
Application	Cisco	Identity Services Engine	2.3\0.298\)	All	All	All
Application	Cisco	Identity Services Engine	2.4	-	All	All
Application	Cisco	Identity Services Engine	2.4	patch1	All	All
Application	Cisco	Identity Services Engine	2.4	patch2	All	All
Application	Cisco	Identity Services Engine	2.4	patch3	All	All
Application	Cisco	Identity Services Engine	2.4	patch5	All	All
Application	Cisco	Identity Services Engine	2.4	patch6	All	All
Application	Cisco	Identity Services Engine	2.4	patch7	All	All
Application	Cisco	Identity Services Engine	2.4	patch8	All	All
Application	Cisco	Identity Services Engine	2.4	patch9	All	All
Application	Cisco	Identity Services Engine	2.4\0.357\)	All	All	All
Application	Cisco	Identity Services Engine	2.6\0.156\)	All	All	All
Application	Cisco	Identity Services Engine	2.7\0.999\)	All	All	All
Application	Cisco	Identity Services Engine	All	All	All	All
cpe:2.3:a:cisco:identity_services_engine:2.3:-:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch1:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch2:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch3:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch5:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch6:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3:patch7:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3(0.298):*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine:2.3\0.298\):*:*:*:*:*:						

```
cpe:2.3:a:cisco:identity_services_engine:2.4:-:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch1:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch2:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch3:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch5:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch6:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch7:::~::~:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch8:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch9:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4(0.357):*:~::~:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4\((0.357\):::*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6(0.156):*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6\((0.156\):::*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7(0.999):*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7\((0.999)\):*:*:*:*:*:
```

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

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

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

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

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

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

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

```
cpe:2.3:a:cisco:identity_services_engine:2.3\((0.298)\):*:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:-:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch1:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch2:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch3:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch5:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4:patch6:::.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:cisco:identity_services_engine:2.4:patch7:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4:patch8:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4:patch9:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4(0.357):*****:
cpe:2.3:a:cisco:identity_services_engine:2.6(0.156):*****:
cpe:2.3:a:cisco:identity_services_engine:2.7(0.999):*****:
cpe:2.3:a:cisco:identity_services_engine:*****:

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 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](#)