



CVE-2020-3467

Published on: 10/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:38 PM UTC

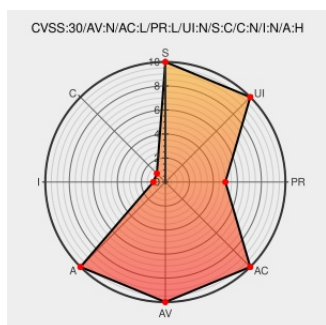
CVE-2020-3467 - advisory for cisco-sa-ise-auth-bypass-uJWqLTZM

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 modify parts of the configuration on an affected device. The vulnerability is due to improper enforcement of role-based access control (RBAC) within the web-based management interface. An

attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to modify parts of the configuration. The modified configuration could either allow unauthorized devices onto the network or prevent authorized devices from accessing the network. To exploit this vulnerability, an attacker would need valid Read-Only Administrator credentials.

CVE-2020-3467 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** 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 - Cisco Identity Services Engine Software** version n/a

CVSS3 Score: **7.7 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References		
Description	Tags	Link
Cisco Identity Services Engine Authorization Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201007 Cisco Identity Services Engine Authorization Bypass 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		
317081 Cisco Identity Services Engine (ISE) Authorization Bypass Vulnerability (cisco-sa-ise-auth-bypass-uJWqLTZM)		

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	2.4.0.357	patch1	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch10	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch11	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch12	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch2	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch3	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch4	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch5	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch6	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch7	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch8	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch9	All	All
Application	Cisco	Identity Services Engine	2.4\0.357\)	All	All	All
Application	Cisco	Identity Services Engine	2.5	All	All	All
Application	Cisco	Identity Services Engine	2.6.0	-	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch1	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch2	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch3	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch5	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch6	All	All

Application	Vendor	Product	Version	Patch	Family	Category
Application	Cisco	Identity Services Engine	2.6\((0.156\)	All	All	All
Application	Cisco	Identity Services Engine	2.7	All	All	All
Application	Cisco	Identity Services Engine	2.7.0.356	patch1	All	All
Application	Cisco	Identity Services Engine	2.7\((0.356\)	All	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch1	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch10	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch11	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch12	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch2	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch3	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch4	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch5	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch6	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch7	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch8	All	All
Application	Cisco	Identity Services Engine	2.4.0.357	patch9	All	All
Application	Cisco	Identity Services Engine	2.4\((0.357\)	All	All	All
Application	Cisco	Identity Services Engine	2.5	All	All	All
Application	Cisco	Identity Services Engine	2.6.0	-	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch1	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch2	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch3	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch5	All	All
Application	Cisco	Identity Services Engine	2.6.0.156	patch6	All	All
Application	Cisco	Identity Services Engine	2.6\((0.156\)	All	All	All
Application	Cisco	Identity Services Engine	2.7	All	All	All
Application	Cisco	Identity Services Engine	2.7.0.356	patch1	All	All
Application	Cisco	Identity Services Engine	2.7\((0.356\)	All	All	All
Application	Cisco	Identity Services Engine	All	All	All	All
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch1:*****:.*:						
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch10:*****:.*:						
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch11:*****:.*:						
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch12:*****:.*:						
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch2:*****:.*:						

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch3:::*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch4:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch5:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch7:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch8:::*.*.*.*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch9:::*.*.*.*.*
```

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

```
cpe:2.3:a:cisco:identity_services_engine:2.5:*:*:*:*:*:*
```

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

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch1:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch2:*:*:*:*:*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch3:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch5:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch6:::*:*.*.*.*.*.*.*.*.*
```

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

```
cpe:2.3:a:cisco:identity_services_engine:2.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7.0.356:patch1:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.7(0.356):*:~::~:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch1:::*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch10:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch11:::*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch12:::*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch2:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch3:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch4:*:*:*:*:
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch5:*:*:*:*.*
```

```
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch6:::*:*:*:
```

cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch7:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch8:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4.0.357:patch9:*****:
cpe:2.3:a:cisco:identity_services_engine:2.4\0.357\):*****:
cpe:2.3:a:cisco:identity_services_engine:2.5:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0:-*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch1:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch2:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch3:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch5:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6.0.156:patch6:*****:
cpe:2.3:a:cisco:identity_services_engine:2.6\0.156\):*****:
cpe:2.3:a:cisco:identity_services_engine:2.7:*****:
cpe:2.3:a:cisco:identity_services_engine:2.7.0.356:patch1:*****:
cpe:2.3:a:cisco:identity_services_engine:2.7\0.356\):*****:
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