

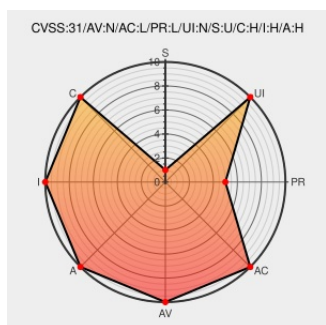


CVE-2020-7174

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7174

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

Certain versions of [Intelligent Management Center](#) from [Hp](#) contain the following vulnerability:

A soapconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07).

CVE-2020-7174 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Document Display HPE Support Center	Vendor Advisory support.hpe.com text/html	MISC support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04036en_us

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	Hp	Intelligent Management Center	All	All	All	All
Application	Hp	Intelligent Management Center	7.3	-	All	All
Application	Hp	Intelligent Management Center	7.3	e0501	All	All
Application	Hp	Intelligent Management Center	7.3	e0503	All	All
Application	Hp	Intelligent Management Center	7.3	e0503p02	All	All
Application	Hp	Intelligent Management Center	7.3	e0504	All	All
Application	Hp	Intelligent Management Center	7.3	e0504p02	All	All
Application	Hp	Intelligent Management Center	7.3	e0504p04	All	All
Application	Hp	Intelligent Management Center	7.3	e0504p2	All	All
Application	Hp	Intelligent Management Center	7.3	e0504p4	All	All
Application	Hp	Intelligent Management Center	7.3	e0506	All	All
Application	Hp	Intelligent Management Center	7.3	e0506p02	All	All
Application	Hp	Intelligent Management Center	7.3	e0506p03	All	All
Application	Hp	Intelligent Management Center	7.3	e0506p07	All	All
Application	Hp	Intelligent Management Center	7.3	e0506p09	All	All
Application	Hp	Intelligent Management Center	7.3	e0605	All	All
Application	Hp	Intelligent Management Center	7.3	e0605h02	All	All
Application	Hp	Intelligent Management Center	7.3	e0605h05	All	All
Application	Hp	Intelligent Management Center	7.3	e0605h07	All	All
Application	Hp	Intelligent Management Center	7.3	e0605h08	All	All
Application	Hp	Intelligent Management Center	7.3	e0605h09	All	All
Application	Hp	Intelligent Management Center	7.3	e0605p04	All	All
Application	Hp	Intelligent Management Center	7.3	e0605p06	All	All
Application	Hp	Intelligent Management Center	7.3	e0701	All	All
Application	Hp	Intelligent Management Center	7.3	e0702	All	All
Application	Hp	Intelligent Management Center	7.3	e0703	All	All
Application	Hp	Intelligent Management Center	7.3	e0703h01	All	All
Application	Hp	Intelligent Management Center	7.3	e0705	All	All


```
opc-2.0.0-mp.intelligent_management_server.7.0.00000opc2. . . . .
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504:*.:.:.:.:
```

cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p02:*:*:*:*:*:

cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p04:*:*:*:*:*:

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p2:*:*:*:*:*
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p4:*:*:*:*:*
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506:*.:*:*:*.*
```

cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p02:*:*:*:*:

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p03:*.:*:*:*.*
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0506p07:::*:*:*.*
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0506p09:*.:.:.:.:
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0605:*:*:*:*:*
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0605h02:*:*:*:*:
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h05:*:*:*:*:*:
```

cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h07:*:*:*:*:*:

```
cpe:2.3:a:hp:intelligent management center:7.3:e0605h08:*.:.:.:.:
```

cpe:2.3:a:hp:intelligent management center:7.3:e0605h09:*.:.:.:.:

```
cpe:2.3:a:hp:intelligent management center:7.3:e0605p04:*.***.***:
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605p06:*:*:*:*:*:
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0701:*.:.:.:
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0702:*.:*:*:*.*
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0703:*:*:*:*.*
```

```
cpe:2.3:a:hp:intelligent_management_center:7.3:e0703h01:*.***.***:
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0705:*.:*:*:*.*
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0705p02:*:*:*:*.*
```

```
cpe:2.3:a:hp:intelligent management center:*:*:*:*:*:*:
```

cpe:2.3:a:hp:intelligent management center:7.3:-:*:*:*:*:*

```
cpe:2.3:a:hp:intelligent management center:7.3:e0501:*.:.:.:
```

```
cpe:2.3:a:hp:intelligent management center:7.3:e0503:*.:.:.:.:
```

cpe:2.3:a:hp:intelligent_management_center:7.3:e0503p02:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p02:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p04:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p2:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0504p4:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p02:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p03:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p07:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0506p09:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h02:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h05:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h07:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h08:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605h09:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605p04:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0605p06:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0701:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0702:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0703:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0703h01:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0705:~::~::~:
cpe:2.3:a:hp:intelligent_management_center:7.3:e0705p02:~::~::~:

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](#)