



CVE-2018-6586

Published on: 03/29/2018 12:00:00 AM UTC

Last Modified on: 01/27/2023 06:19:00 PM UTC

CVE-2018-6586

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Api Developer Portal](#) from [Ca](#) contain the following vulnerability:

CA API Developer Portal 3.5 up to and including 3.5 CR6 has a stored cross-site scripting vulnerability related to profile picture processing.

CVE-2018-6586 has been assigned by vuln@ca.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **CA Technologies - CA API Developer Portal** version **3.5 CR7**

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CA API Developer Portal Input Validation Flaws Let Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTrack 1040603

Patch
Vendor Advisory
web.archive.org
text/html
Inactive Link Not Archived

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	Ca	Api Developer Portal	3.5	All	All	All
Application	Ca	Api Developer Portal	3.5	cr1	All	All
Application	Ca	Api Developer Portal	3.5	cr2	All	All
Application	Ca	Api Developer Portal	3.5	cr3	All	All
Application	Ca	Api Developer Portal	3.5	cr4	All	All
Application	Ca	Api Developer Portal	3.5	cr5	All	All
Application	Ca	Api Developer Portal	3.5	cr6	All	All
Application	Ca	Api Developer Portal	3.5	All	All	All
Application	Ca	Api Developer Portal	3.5	cr1	All	All
Application	Ca	Api Developer Portal	3.5	cr2	All	All
Application	Ca	Api Developer Portal	3.5	cr3	All	All
Application	Ca	Api Developer Portal	3.5	cr4	All	All
Application	Ca	Api Developer Portal	3.5	cr5	All	All
Application	Ca	Api Developer Portal	3.5	cr6	All	All

```
cpe:2.3:a:ca:api_developer_portal:3.5:*:*:*:*:*:*
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr1:*:*:*:*:*:
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr2:*:*:*:*:*:
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr3:*:*:*:*:*
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr4:*:*:*:*:*:
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr5:*:*:*:*:*:
```

```
cpe:2.3:a:ca:api_developer_portal:3.5:cr6:*:*:*:*:*:
```

```
one:2 3:2:carani developer portal:3 5:*****.
```

cpe:2.3:a:ca:api_developer_portal:3.5:1:.*.*.*.*
cpe:2.3:a:ca:api_developer_portal:3.5:cr1:.*.*.*.*:
cpe:2.3:a:ca:api_developer_portal:3.5:cr2:.*.*.*.*:
cpe:2.3:a:ca:api_developer_portal:3.5:cr3:.*.*.*.*:
cpe:2.3:a:ca:api_developer_portal:3.5:cr4:.*.*.*.*:
cpe:2.3:a:ca:api_developer_portal:3.5:cr5:.*.*.*.*:
cpe:2.3:a:ca:api_developer_portal:3.5:cr6:.*.*.*.*:

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