

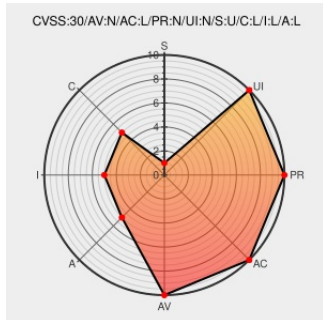


CVE-2020-2786

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 10/14/2022 06:27:00 PM UTC

CVE-2020-2786

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

Certain versions of [Outside In Technology](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability

can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).

CVE-2020-2786 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Oracle Corporation - Outside In Technology** version = **8.5.4**

CVSS3 Score: **7.3 - HIGH**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - April 2020	Vendor Advisory www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2020.html

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	Oracle	Outside In Technology	8.5.4	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
Application	Oracle	Outside In Technology	8.5.4	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
cpe:2.3:a:oracle:outside_in_technology:8.5.4:*:*:*:*:*:						
cpe:2.3:a:oracle:outside_in_technology:8.5.5:*:*:*:*:*:						
cpe:2.3:a:oracle:outside_in_technology:8.5.4:*:*:*:*:*:						
cpe:2.3:a:oracle:outside_in_technology:8.5.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

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](#)