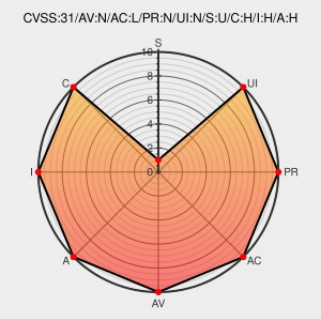
CVE-2020-1745

Published on: 04/28/2020 12:00:00 AM UTC

Last Modified on: 09/14/2021 02:00:00 PM UTC

CVE-2020-1745

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Undertow from Redhat contain the following vulnerability:

A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.

CVE-2020-1745 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **undertow-io** - **undertow** version **<= 2.0.29.Final**

CVSS3 Score: 9.8 - CRITICAL

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

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
No Description Provided	Not Applicable www.cnvd.org.cn text/html Inactive Link Not Archived	MISC www.cnvd.org.cn/webinfo/show/5415
CVE-2020-1938: Apache Tomcat AJP Connector Remote Code Execution Vulnerability Alert • InfoTech News	Not Applicable meterpreter.org text/html	MISC meterpreter.org/cve-2020-1938-apache-tomcat-ajp-connector-remote-code-execution-vulnerability-alert/
CVE-2020-1938: Ghostcat - Apache Tomcat AJP File Read/Inclusion Vulnerability (CNVD-2020-10487) - Blog | Tenable®	Not Applicable www.tenable.com text/html	MISC www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cnvd-2020-10487
1807305 – (CVE-2020-1745) CVE-2020-1745 undertow: AJP File Read/Inclusion Vulnerability	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1745

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Undertow	All	All	All	All

cpe:2.3:a:redhat:undertow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tomcat - CVE-2020-1745: bugzilla.redhat.com/show_bug.cgi?i…	2021-09-14 16:46:53

← Previous ID

Next ID→