CVE-2021-20220

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-20220
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-23 18:15:00 UTC
Updated	2022-02-22 14:53:00 UTC
Description	A flaw was found in Undertow. A regression in the fix for CVE-2020-10687 was found. HTTP request smuggling related to C

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Redhat	Undertow	All	All	All	All
Application	Redhat	Undertow	All	All	All	All

References

Reference	Source	Link
CVE-2021-20220 Undertow Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
1923133 – (CVE-2021-20220) CVE-2021-20220 undertow: Possible regression in fix for CVE-2020-10687	MISC	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982232 Java (maven) Security Update for io.undertow:undertow-core (GHSA-qjwc-v72v-fq6r)