Advisory Alert

Alert Number: AAA20210504 **Date:** May 4, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	BIND security update

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	BIND security update (CVE-2021-25215)
Description	DNAME records provide a way to redirect a subtree of the domain name tree in the DNS. A flaw in the way DNS server (named) processes these records may trigger an attempt to add the same RRset to the ANSWER section more than once. This causes an assertion check in BIND to fail. When a vulnerable version of “named” receives a query for a record triggering the flaw described above, the “named” process will terminate due to a failed assertion check.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.4 x86_64 Red Hat Enterprise Linux Server - TUS 7.4 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.4 ppc64leRed Hat Enterprise Linux Server - Update Services for SAP Solutions 7.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:1479 https://access.redhat.com/security/cve/CVE-2021-25215?extIdCarryOver=true&sc_cid=701f2000001OH7JAAW

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.