Advisory Alert

Alert Number: AAA20220815 **Date:** August 15, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PostgreSQL	**HIgh**	Arbitrary Code Execution Vulnerability.

Description

Affected Product	**PostgreSQL**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability. (CVE-2022-2625)
Description	PostgreSQL has released a patch update addressing an Arbitrary Code Execution vulnerability that exist because of the extension scripts replace objects not belonging to the extension. To carry out this attack, an attacker requires permission to create non-temporary objects in at least one schema, ability to lure or wait for an administrator to create or update an affected extension in that schema and ability to lure or wait for a victim to use the object targeted in CREATE OR REPLACE or CREATE IF NOT EXISTS. This vulnerability affects to the both PostgreSQL-bundled and non-bundled extensions. PostgreSQL highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	PostgreSQL version 10, 11, 12, 13, 14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2022-2625/

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.