CERT Vulnerability Data Archive and Tools

The Data

The CERT Vulnerability Data Archive contains nearly all of the non-sensitive vulnerability data collected by the CERT/CC, from the inception of the vulnerability notes database (approximately May 1998) to the date the archive was prepared, as noted above in the Change Log.

Since roughly 2004, the United States Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) has funded the vulnerability analysis and coordination work that includes this vulnerability data and the publication of Vulnerability Notes.

This data is incomplete. All records (reports) should have an ID, title, and creation date. Only some (~6%) of the reports have been analyzed, coordinated, written up, and published as Vulnerability Notes.

Most of the reports are in a preliminary state, with blank or default field values. Few fields are consistently entered across the entire data set. It is generally inappropriate from an analysis perspective to draw conclusions from incomplete and inconsistent data. You have been warned.

There are two sets of data, vulnerability reports and vendor records. A published Vulnerability Note is made up of one vulnerability report and one or more vendor records.

The Tools

At this time we have no plans to provide any full-fledged applications. Instead we are offering a simple `VulDb()` Python class that can load the vulnerability data contained in the archive. It's up to you to decide how to use it. Anyone with some basic Python skills should be able to make use of this package.

For more information, and to download the data and tools, see the links at right.

More information about the Vulnerability Data Archive

Blog post announcing the Vulnerability Data Archive.

Download

The data and tools are both available via GitHub. Follow the links below for further instructions and to download them.

Vulnerability Data Archive

GitHub

Vulnerability Data Archive Tools

GitHub