What's New

- New
- Fixed
- Improved
- Removed
- Known bug

Version 1.1.0.1 **January 3, 2023**

This is first updated feature release. Also some improvements and bug fixes are included. In the list below an overview of the features included in the first release of the **V-Check** application:

- CVE details: Added a section with information from the so-called Known Exploited Vulnerabilities (KEV) catalog as maintained by the US CISA (Cybersecurity & Infrastructure Security Agency, www.cisa.gov). This information displayed comes via the API of the NVD (nvd.nist.gov)
- Added the option to filter on only the vulnerabilities that is known exploited. This data comes via the US CISA as supplied via the NVD API.
- Added haptic feedback on the buttons of the CVE list view. Haptic feedback can be enabled/disabled in the settings menu.
- Added an unread indicator and filter option. When new or updated CVE entries are loaded an unread indicators (small blue circle next to CVEid in List view) is added. This resets as soon as the CVE is selected to show its details. In the filter sheet an option is added to filter on the unread setting. Double tap on count summary section will reset all unread flags.
- Added the option to setup your own NVD API key. This must be a key that is supplied by the nvd.nist.gov site. This can be useful in case an API key gets overloaded, or simply does not work anymore.
- Added a progress bar to show the download of CVE records status. The progress bar only shows when there is actually a download ongoing.
- Added a CVE download sheet with a number of options to set what needs to be downloaded from the NVD database. The number of options are planned to grow in subsequent releases. Now 2 options are available: 1. Full and 2. Incremental. For option Full, a full data download from the NVD CVE database will be done. For option 2. Incremental the CVEs that are modified in a specific timeframe will be downloaded. The startpoint is determined by the CVE with the most recent modification date as hold in the local database. The endpoint will be (maximal) 120days later.
- End date in CVE filter window now ignores the time. In version 1.0.0, the time was also used. Resulting in the fact that not all records where shown after the time the ends-at-date was set for the last time.
- Fixed color scheme for "ADJACENT_NETWORK" in access vector for the CVSS2 model.
- Fixed search on CVE list to be case insensitive for the CVEid field.

Version 1.0.0.1 **December 30, 2022**

This is the initial feature release of the **V-Check** application. **V-Check** stands for Vulnerability Check, where vulnerability is in the context of cybersecurity. It provides an overview of the so-called Common Vulnerabilities and Exposures (CVE). It also includes all related details like for Common Weaknesses (CWE), Platforms (CPE) and detailed CVSS (Common Vulnerability Scoring System) scoring information.

Note: V-Check uses data from the NVD (nvd.nist.gov) and MITRE (cwe.mitre.org), but is not endorsed in any way by either.

In the list below an overview of the features included in the first release of the **V-Check** application:

- CVE overview: This view provides a comprehensive list of the CVE's, including the short description, CVSS score, publish- and modification dates. And by selecting one of the entries, full details will be provided.
- CVE details: A full detailed CVE view that provides details of the CVSS score, the related CWE (Common Weaknesses Enumeration), CPE (Common Platform Enumeration) and References.
- CVE filter: This provides extensive searching and filtering options. CVEs can be filtered and sorted from the local database on several parameters. The filter settings will be maintained in persistent storage over session.
- CVE search: A quick and easy search on the filtered CVE list in the CVE ID or description field. This to fine tune further searching.
- The CVE data is maintained in a local (SQL-based) database that gets filled with the data pulled from the NVD site. In an easy pull-to-refresh way data will be updated to the latest information available.
- Under settings the database can be cleaned and/or re-initialised. The database enables that, after initialisation, the app can also be used without an internet connection. Though obviously for updates it needs a internet connection to update and load the database.
- CWE overview: This overview provides a list of Common Weakness Enumeration items. A more detailed description, including an extended description are provided as well.
- CWE details: This provides the more detailed description of the CWE item. It includes the description and extended description. More information will be added in subsequent releases.
- CWE search: An easy search function to search the CWE list in the CWE ID or CWE description fields.
- Settings - General : here 3 items can be found: About, Release Notes (this document) and how to issue a Support request.
- Settings - User Interface: here the appearance (dark-, light, system mode) can be changed. The App fully supports dark mode. Next the App Icon can also be adjusted as to your best liking. In this release 3 color variants are included: red, purple and blue.
- Settings - Database. Under this function specific database management can be done. The database maintains all information pulled over the internet from either the NVD or MITR websites. Actions include: clearing the database (i.e. making it empty) and initialisation with a full fetch of data from the NVD and/or MITRE.
- Share Information: from both the CVE and CWE list information can be shared (exported) via a *share sheet*. In that way information can be shared to e.g. e-mail, todo application, notes etc. In fact any application that supports share sheet.