TITANIA | Technical brief

Vulnerability reporting against Cisco devices with Nipper InfraSight

Nipper InfraSight provides a plugin to generate a vulnerability report against a device. The plugin does this by extracting the firmware version from the device configuration, and then searching the vulnerability database for the vulnerabilities known to be relevant for that firmware version.

The vulnerability database used is the NIST NVD database, now distributed in JSON format. While NIST endeavour to keep this database as up to date as possible, it can sometimes be behind official CERT CVE declarations, and this can lead to apparent inaccuracy.

However, a further issue arises with Cisco devices, and this derives from the way Cisco version numbering works and the fact that Cisco state that it is not possible to distinguish chronological order from those version numbers (see detailed description in the next section). This means that it is not possible to perform the range matching specified in the NVD database and leads to errors in the vulnerability reporting.

To overcome this limitation Titania now offer two methods to report on Cisco devices. Firstly, the NVD reporting plugin remains, and operates as before, which can lead to the above described issues. Secondly we have developed a new plugin only applicable to Cisco devices, PSIRT (which refers to the Product Security Incident Response Team). This plugin takes vulnerability data for a specified version directly from Cisco, solving the version number chronology problem and has the most up to date vulnerability data from Cisco that will be supplied to NIST.

Titania recommend therefore that as of Nipper InfraSight version 2.7 users adopt the PSIRT plugin for Cisco devices, selecting that report at Stage 2 of the audit process.

This may require a change in the approved audit process for some customers, but the change delivers accurate vulnerability reporting that is not possible using the NVD data, and Cisco version numbering.

Titania elected to offer this capability as a separate plugin, as the data used is not derived from NVD, and it would be confusing to interpret reports where, for some devices, the data was taken from NVD and for others from another source.

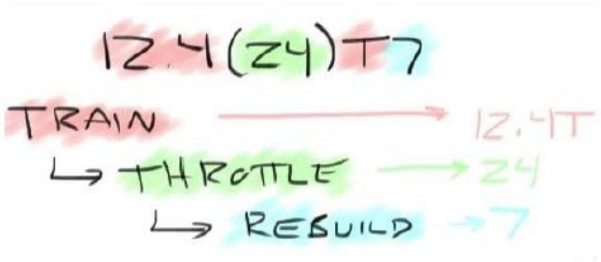
Titania products are renowned for their accuracy, and the inclusion of the PSIRT report for Cisco devices further improves this.

Detailed description of the issue solved

In the below example, we have chosen CVE-2018-0189 The matching data in the NVD database states that all versions up until 15.2.(5)e1 are susceptible to this vulnerability.

“cpe_match”: [
{
“cpe23Uri”: “cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*”,
“versionEndExcluding”: “15.2\\(5\\)e1”,
“vulnerable”: true
}
],

The Cisco version number system is described here, where they describe the component parts of the version number as in Figure 2 below



So, in our example that is Train 15.2T, throttle 5, rebuild E1 The following is taken directly from the Cisco reference.

Trains

The IOS Train is something like major version number if you think about conventional software nomenclature. This is where the foundation of an IOS feature set is established. More features can be added later when a new throttle is created.

Throttles

IOS Throttle is roughly a minor version number where some new features and bug fixes may have been added. For Cisco IOS the general rule of thumb is that new features are not added “mid-throttle”. In other words, when new features need to be added, they would be added when a new throttle is started.

Rebuilds

IOS Rebuilds typically consist of bug fixes. Adding new features to a rebuild is generally avoided but it does happen sometimes. With rebuilds it can be confidently stated that one version of IOS is more recent than another. For example, 12.4(24)T7 is newer than 12.4(24)T5.

Conclusion

So, although it is possible to use Rebuild number with Train and Throttle constant, to determine the chronological build order and therefore the CVE susceptibility as described by the range in the CPE data, this is of limited use. Cisco state that “Within a platform you still can’t reliably use IOS version to determine what is most recent.”

In our example case consider a device Cisco IOS_XE with version number 15.2(7)E0s. There is no reliable way to determine if 15.2(7)E0s was released before or after 15.2(5) e1, therefore no way to tell if that version is vulnerable to CVE-2018-0189. This is because the Train/Throttle numbers are not common across the compared versions. As it is not possible to correctly determine the range comparison, this can lead to false positives (erroneously flagging CVE vulnerabilities), or false negatives (omitting to report vulnerabilities).

The Cisco PSIRT data takes care of this chronology issue, and correctly tags the CVE against the operating system version numbers, so there is no range calculation to perform.