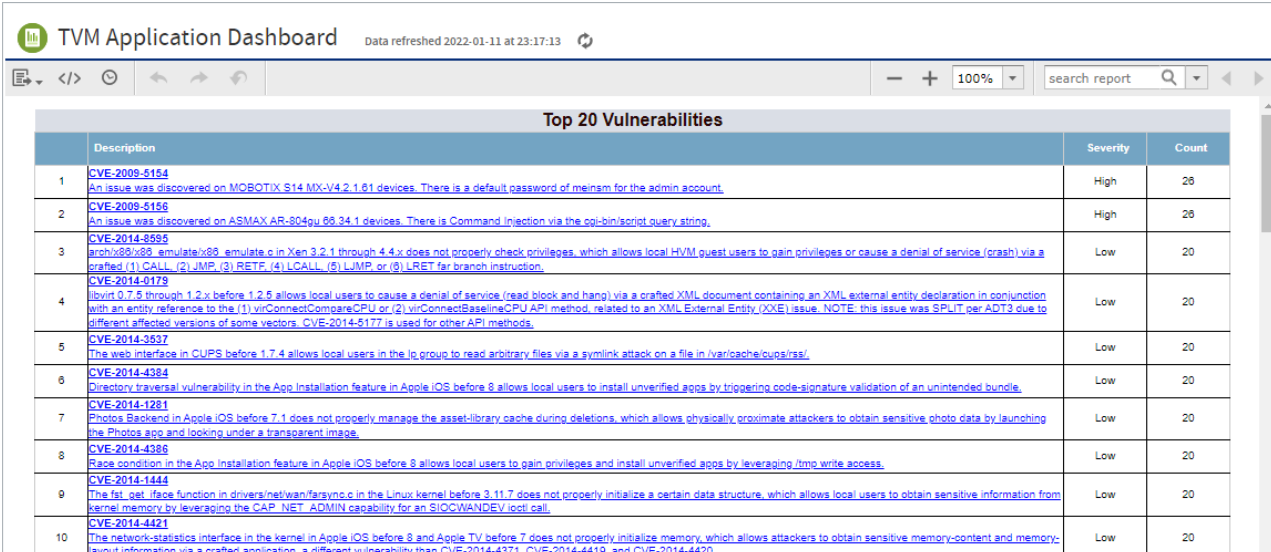


About Threat Management

Threat management means being aware of known [vulnerabilities](#) that may apply to your entities and technologies.

The National Vulnerability Database (NVD) tracks thousands of vulnerabilities, most identified by a unique CVE (Common Vulnerabilities and Exposures) number.



The screenshot shows the TVM Application Dashboard interface. At the top, it says "TVM Application Dashboard" and "Data refreshed 2022-01-11 at 23:17:13". Below this is a navigation bar with a search report field. The main content area is titled "Top 20 Vulnerabilities" and contains a table with the following data:

	Description	Severity	Count
1	CVE-2009-5154 An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. There is a default password of meism for the admin account.	High	28
2	CVE-2009-5156 An issue was discovered on ASMAX AR-804gu 66.34.1 devices. There is Command Injection via the cgi-bin/script query string.	High	28
3	CVE-2014-8555 arch/x86/x86_emulate.c in Xen 3.2.1 through 4.4.x does not properly check privileges, which allows local HVM guest users to gain privileges or cause a denial of service (crash) via a crafted (1) CALL, (2) JUMP, (3) RETF, (4) LCALL, (5) LJMP, or (6) LRET far branch instruction.	Low	20
4	CVE-2014-0179 libvirt 0.7.5 through 1.2.x before 1.2.6 allows local users to cause a denial of service (read block and hang) via a crafted XML document containing an XML external entity declaration in conjunction with an entity reference to the (1) virConnectCompareCPU or (2) virConnectBaselineCPU API method, related to an XML External Entity (XXE) issue. NOTE: this issue was SPLIT per ADT3 due to different affected versions of some vectors. CVE-2014-5177 is used for other API methods.	Low	20
5	CVE-2014-3637 The web interface in CUPS before 1.7.4 allows local users in the lp group to read arbitrary files via a symlink attack on a file in /var/cache/cups/ps/.	Low	20
6	CVE-2014-4384 Directory traversal vulnerability in the App Installation feature in Apple iOS before 8 allows local users to install unverified apps by triggering code signature validation of an unintended bundle.	Low	20
7	CVE-2014-1281 Photos Backend in Apple iOS before 7.1 does not properly manage the asset-library cache during deletions, which allows physically proximate attackers to obtain sensitive photo data by launching the Photos app and looking under a transparent image.	Low	20
8	CVE-2014-4386 Race condition in the App Installation feature in Apple iOS before 8 allows local users to gain privileges and install unverified apps by leveraging /tmp write access.	Low	20
9	CVE-2014-1444 The fst_get_iface function in drivers/net/wan/farsync.c in the Linux kernel before 3.11.7 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability for an SIOCWANDEV ioctl call.	Low	20
10	CVE-2014-4421 The network-statistics interface in the kernel in Apple iOS before 8 and Apple TV before 7 does not properly initialize memory, which allows attackers to obtain sensitive memory content and memory layout information via a crafted application, a different vulnerability than CVE-2014-4371, CVE-2014-4419, and CVE-2014-4420.	Low	20

The Threat & Vulnerability Manager Application Dashboard.

Not all vulnerabilities will apply to your organization. The NVD and other subscription feeds, such as VeriSign iDefense Labs, provide vulnerability definitions (VD). When a VD targets your entities or [technologies](#), the system identifies a vulnerability instance (VI). VIs can be inferred (reported by a feed) or actual.

RiskVision works with vulnerability scanners, such as Qualys, that identify vulnerability instances. RiskVision can also create VIs on its own, based on VDs and the [technologies catalog](#) known as the Common Platform Enumeration (CPE). VIs are usually identified by CVE numbers. The same VI may be reported more than once for a given entity.