ordr

MODERNIZING YOUR VULNERABILITY MANAGEMENT PROGRAM IN THE AGE OF UNMANAGED, CONNECTED DEVICES

Introduction

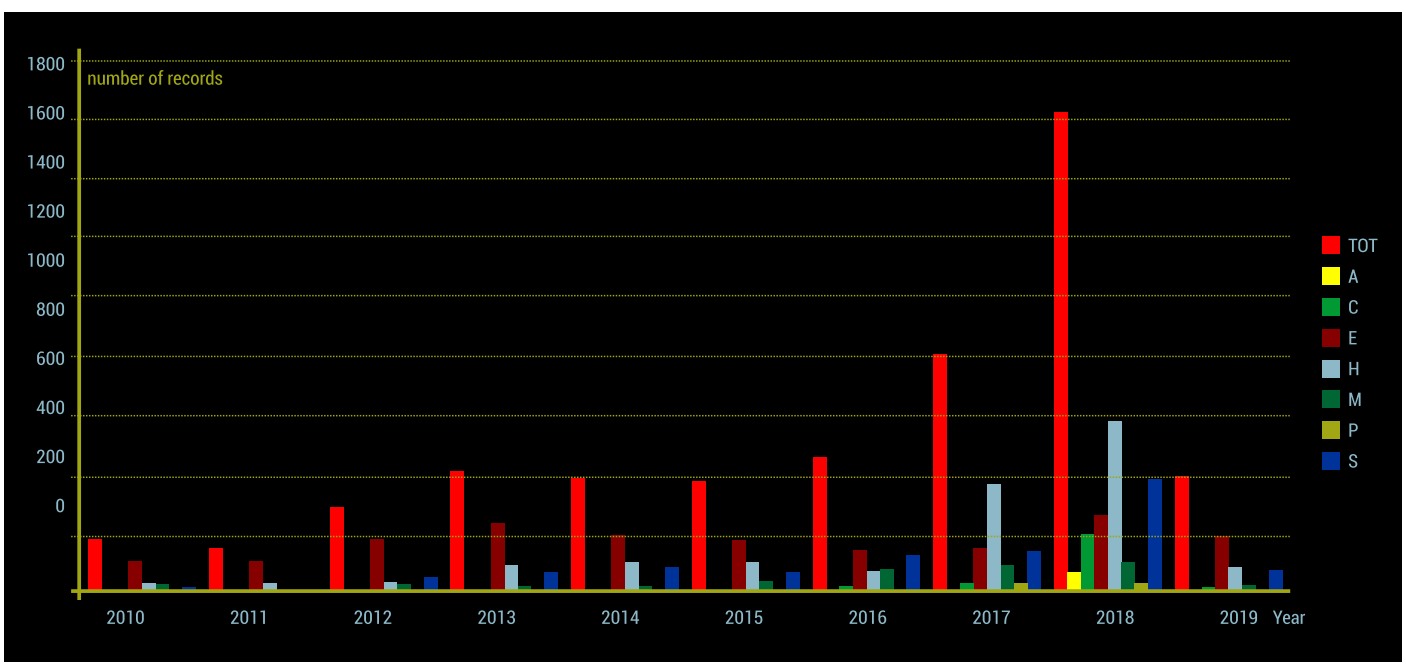
Vulnerability Management is one of the most critical yet challenging aspects of security facing organizations today. Security professionals across all industries have long known that finding and mitigating these weaknesses is one of the most proactive things an organization can do to avoid the damage and loss.

However, these security best intentions have hit a wall of real-world challenges. Organizations face far more vulnerabilities than ever before, with the rate of new CVEs more than doubling in recent years. Organizations likewise have more devices to protect than ever before, often segmented into more and more subnets. Teams are overwhelmed with vulnerabilities, and the complexity makes it easy for devices and network segments to slip through the cracks.

Worse, many of the most critical devices such as IoT, OT, and medical devices are not discovered, seen, or properly profiled by traditional vulnerability scanners. There are plenty of examples of cyber analysts disrupting the operation of IoT, OT, and medical devices by doing a vulnerability scan on these devices. Even if vulnerabilities are found on these devices, IT and security staff often lack the context of the device that they need in order to properly prioritize addressing vulnerabilities on the devices.

Getting Control of the Device Side of Vulnerabilities

While keeping pace with the constant flow of new vulnerabilities has always been a daunting task, hard data is available that shows why the problem has gotten considerably worse in recent years, particularly when it comes to connected device vulnerabilities. By analyzing Common Vulnerability Enumerations (CVEs), we can see an explosion in the number of IoT vulnerabilities that far outpaces the industry average. A 2020 academic study found that the yearly rate of new IoT CVEs nearly quadrupled between 2016 and 2018. Note that the chart below only contains data from the first quarter of 2019.



The chart, developed by Blinowski, Grzegorz & Piotrowski, Paweł. (2020), provides CVE-based classification of vulnerable IoT systems.

Device vulnerabilities are also incredibly widespread. The Ripple20 vulnerabilities consist of 19 vulnerabilities found in the TCP/IP stack used in everything from printers to infusion pumps to industrial control systems. The CDPwn vulnerabilities affecting Cisco's Cisco Discovery Protocol (CDP) likewise affected tens of millions of enterprise devices.

Unfortunately, the increase in connected device vulnerabilities has translated into real-world attacks. A 2019 security report from F-Secure found that IoT attacks have increased by roughly 300%. Mirai, a notorious IoT botnet, likewise nearly doubled its activity and shifted to more enterprise targets. Other malware such as Silex has focused on disabling or "bricking" IoT devices, which can have devastating impacts on clinical and different high-value environments.

Common Vulnerability Management Challenges

Vulnerability scanners are an essential part of every organization's security practice. However, in order to do their job, they need to know what to scan, and just as importantly, what not to scan. Additionally, scanners typically don't know what they've missed. With staff already busy and overworked, it is all too easy for scans to miss important devices or entire segments of a network. Specific challenges include:

Missing Important Network Segments - Network-based vulnerability scans naturally follow the rules of the network and need to be told what subnets and IP ranges to scan. As modern networks become increasingly segmented, it can be easy for scanners to miss entire segments of the network.

Missing Devices - Vulnerability scans naturally represent a point in time, and devices can be missed during a scan for a variety of reasons. A system could have been temporarily offline or a device could have been out of the office on the day of the scan. These can mean that critical devices can be exposed for extended periods of time without the security team's knowledge.

Manual Inclusion or Exclusion Rules - Scanning tools typically only see a host as an IP address. However, staff may not want all devices to be scanned or to be scanned with the same intensity. Since scanners don't know one device from another, teams must manually create lists to target devices appropriately.

Connected Device Gaps in Vulnerability Management

The combination of many vulnerabilities, many affected connected devices, and active real-world attacks creates a recipe for considerable enterprise risk. The problem is that these vulnerabilities are typically a blind spot to an organization's vulnerability management program in the following ways:

Missed Connected Device Vulnerabilities – Traditional vulnerability scanners focus heavily on software and application layer vulnerabilities, while connected and IoT device vulnerabilities are typically embedded in the device itself. Additionally, IoT devices often utilize a variety of open source components such as those that were behind the Ripple20 vulnerabilities.

Dangers in Scanning IoT Devices – Organizations may not want to scan specific IoT devices for vulnerabilities since the scan itself could possibly disrupt the operation of the device (ie. medical devices).

Lack of Operational Context – Even if a vulnerability is found in an IoT device, traditional scanners today often lack the rich context to power the appropriate workflow.

How Ordr Helps

Ordr closes the connected device vulnerability gap, giving IT and Security teams insight into vulnerabilities that would typically be missed while arming them with the critical context needed in order to make appropriate remediation decisions.

Passive Identification of IoT Devices and Vulnerabilities

Ordr gathers information on all devices in the environment by passively analyzing traffic on the network. This includes IoT, OT, IoT, IoMT as well as traditional devices such as laptops and servers. Through Deep Packet Inspection (DPI) Ordr is able to automatically identify devices by their type and function as well as high fidelity details such as the version, model number, and even version of operating system. Knowing a device is running an unsupported OS like Windows XP is critical to truly understanding the risk of that device.

Ordr then maps these device details to industry vulnerabilities based on integration with a variety of industry-specific feeds such as the ICS-CERT database, ICSA for ICS-CERT advisories, as well as health care vulnerability feeds including the FDA recall database, ICS—CERT, H-ISAC, and support for MDS2 forms. Ordr's deep packet inspection of traffic can additionally identify a variety of additional device weaknesses such as devices using expired certificates.

This approach gives organizations insight into specific connected device vulnerabilities, all without directly interacting the device. This gives organizations important insight that can be used to include or exclude devices into future scans. Instead of seeing a device simply as an IP address, teams can recognize critical devices that they may want to exclude from an automated scan to ensure that the scan doesn't cause an interruption in service.

Clinical and Manufacturing Risk Context

Most organizations have far more vulnerabilities than they have the time and staffing resources to patch. As a result, it is critical that teams be able to quickly prioritize the vulnerabilities that present the greatest risk to the organization. This is particularly important in clinical and other high-value environments.

Ordr gives a wealth of threat and clinical context to help teams easily find the devices that need priority attention. First, the Ordr platform contains built in IDS capabilities. This allows the system to directly correlate devices that are vulnerable and are also under attack from threats. This gets staff to an immediate contextual answer without having to correlate data in multiple separate systems or a SIEM.

Next, the solution prioritizes devices based on environmental traits including the value of the device, its location, and the content on the device itself. For example, a vulnerable device could be prioritized if it contains PHI. Likewise, devices can be prioritized based on its type and manufacturer and where it is, for example, a respirator or infusion pump that is in an acute care unit. This allows security staff to see vulnerabilities in terms of the overall risk they present to an organization's mission.

Ordr: The Missing Piece In Vulnerability Management

The Ordr System Control Engine (SCE) gives enterprises the proper solution to ensure that their vulnerability management program is both comprehensive while also being pragmatic and efficient. With easily deployed passive visibility into traffic, Ordr improves vulnerability management in the following ways:

Full Visibility – Through passive traffic analysis, Ordr is able to identify all of an organization's devices. This can reveal devices and network segments that might be missed by scanners.

Automatically Identify Devices by Type – Identify all types of devices, including IoT, OT, and IoMT. Teams will know exactly where all their devices are and instantly distinguish a security camera from a medical imaging system from a regular end user laptop.

Find Device and Industry-Specific Vulnerabilities – Complement traditional software vulnerability scanning with device-specific scans to identify recalls and vulnerabilities in IoT, OT, and IoMT.

Prioritize Based on Industry-Specific Risk Context – Prioritize high-value devices, high-value areas such as clinical and manufacturing environments, devices that contain sensitive data such as PHI, devices that have known vulnerabilities, and more.

Integrate Ordr with Your Existing Vulnerability Scanner – Combining Ordr's unique device intelligence with advanced vulnerability intelligence provides organizations with the ultimate solution to efficiently manage risks while reducing service disruption and time to remediate.

In addition to addressing connected device vulnerabilities, Ordr works with your existing vulnerability scanners and tools to make vulnerability management far more comprehensive, efficient, and unified. Ordr can bridge the gap between tools to ensure that staff always have a unified view of all vulnerabilities in their environment. Next, with full visibility over the environment, Ordr can identify any gaps in the organization's scanning and either scan them directly or schedule the appropriate scans by other tools.

Conclusion

While most modern organizations recognize the critical importance of vulnerability management, the sheer scale of the job can make it hard for staff to keep up. The growth of critical connected devices in organizations has added to an already complex landscape and created a new attack surface that is often invisible to traditional vulnerability management tools.

Ordr solves these challenges. The solution's built-in expertise automatically identifies vulnerabilities in IoT, OT, and IoMT devices that aren't seen by traditional scanners. Each vulnerability comes with deep insight into the device and clinical and threat-based contexts so that teams quickly find the devices that need priority attention. And with visibility into all connected devices, the platform makes the perfect complement to any existing vulnerability management program.

To learn more about the Ordr platform, please contact the Ordr team at www.ordr.net.