RAPID7

RESEARCH

Practical Guidance for Security Teams

From the 2021 Vulnerability Intelligence Report

Despite patchy vendor guidance for some vulnerabilities in this report, the tried-and-true pieces of guidance in this section can afford security teams time and assist them in identifying suspicious or malicious activity. Though each security program—even those within the same organization—has different maturity and capability, these steps are battle-tested to make compromising organizations as hard as possible for attackers.

Rapid7 researchers publish analysis for high-priority vulnerabilities in Rapid7's community vulnerability assessment platform, AttackerKB. These analyses often include sample proof-of-concept code and indicators of compromise in addition to exploitation timelines and attack chain analysis. Those who wish to subscribe to notifications for formal Rapid7 analysis in AttackerKB can create a free account. Blogs on emergent threats are published here.

Get good at the basics of vulnerability management.

Robust vulnerability management is the foundation of any successful IT security program. Without the proactive discipline of vulnerability management and strong routine patch management practices developed during days of relative calm, it is nearly impossible to up-level to effective emergency patching in times of crisis. Incident response measures in the absence of proactive vulnerability management are also likely to be frenetic firefighting that is reactive and ineffective.

Within vulnerability management, asset inventory and patch management are foundational activities to get right. Good asset visibility is essential to many aspects of IT management. It's difficult to act quickly and decisively in a crisis if you don't know which technologies are present in your environment or where they live in your tech stack. Identify and catalog your critical and exposed systems, including security boundary devices, internet-facing load balancers, devops tooling and pipeline solutions, and virtualization infrastructure. For more fundamentals, read Rapid7's guidance on security program basics.

Limit and monitor your internet-facing attack surface area.

Understanding attack surface area and critical network entry points saves time when severe vulnerabilities surface in internet-facing technologies. Exploitation of many of the CVEs in this report—including some of those exploited in zero-day attacks—can be slowed down by limiting internet exposure of critical applications and management interfaces. Pay particular attention to security gateway products such as VPNs and firewalls, as well as anything else that's exposed by common practice or necessity. CVE-2021-22893 and CVE-2021-20016 are noteworthy examples.

Management and administrative interfaces should never be exposed to the public internet. The same goes for domain controllers and any other assets that organizations would not want an external attacker to be able to probe, such as IoT devices unwittingly exposed online. Audit internet-exposed attack surface area regularly, including via external penetration tests, if possible.

Ensuring that (preferably aggregated) logging is set up across networks and hosts will save some time during active threat events. There are several community-driven signature repositories and low-cost rulesets that can give security teams at least basic visibility into potential intrusions in their environments, along with a plethora of commercial solutions. Knowing ahead of time what kind of visibility you have into suspicious events will drive faster and more effective responses during critical situations.

Harden critical systems.

Harden critical products against low-skill and opportunistic attacks. Your virtualization and network infrastructure solutions should be isolated not only from the internet, but from as many internal systems as possible. Make it difficult for attackers to get to the applications that are central to the management of your network and operations.

While it may seem basic, hardening includes ensuring you've changed all default and administrative passwords in technology you implement to be complex and non-standard. Software and solutions you rely on in your environment may have undocumented service or administrative users—though we hope none of these have hard-coded passwords. Thorough review and segmentation will slow down attackers. Implement multi-factor authentication (MFA) and monitor authentication events for remote logins.

Define both a regular patching cycle and emergency zero-day patching procedures.

The window for effective patching has decreased in the past two years. Fifty-percent of the vulnerabilities in this report were exploited within seven days of disclosure. It is essential that organizations have emergency patching procedures and incident response playbooks in place in addition to a clearly defined, regular patch cycle that prioritizes actively and widely exploited CVEs. Without an understood, standardized mechanism for driving aligned emergency action, you're at much higher risk from these increasingly frequent events.

In addition to regular and emergency patching procedures, organizations should ensure they keep current with operating system-level updates, such as Microsoft's **Cumulative Updates** for Windows systems. Failing to ensure timely installation of Cumulative Updates may mean that you are unable to quickly install out-of-band security patches when sudden attacks occur.

The same principle applies to all operating system-level patches, no matter the platform; OS-level vulnerabilities are a boon to attackers, even if they are not exposed to the internet.

Network edge devices (network pivots) continue to be popular and frequently exposed attack surface area. The same goes for network infrastructure targets that offer attackers the ability to compromise downstream devices or resources (e.g., virtualization infrastructure) and email servers like Microsoft Exchange. These categories of software and firmware should adhere to a zero-day patch cycle wherever possible, meaning that updates and/or downtime should be scheduled as soon as new critical or high-severity advisories are released.

As of late 2021, the U.S. Cybersecurity and Infrastructure Agency (CISA) has a list of known-exploited vulns (**KEV**), which they are updating on a regular basis. While the patching deadlines in the KEV list are aimed at government agencies and federal contractors, it's a good idea for non-government organizations to track that guidance and those SLAs closely.

Leverage resources on ransomware prevention and readiness.

The rise of ransomware has changed the security landscape, and organizations should be prepared to implement multilayered defenses against ransomware threats. The Institute for Security and Technology has a comprehensive **framework** for ransomware prevention and readiness developed in partnership with industry experts, **including Rapid7**. CISA also has **in-depth guidance** on readiness and response. Rapid7 has additional ransomware resources **here** and regularly **writes about** ransomware detection and prevention tactics.

Development pipelines are targets—and developers can be, too.

Rapid7's security teams published an in-depth list of **practices for protecting development pipelines** from supply chain attacks. This list covers topics from version control and job-specific credentials for CI jobs to secrets and hash management. It also includes detection and response techniques.

Defense in depth is a more effective strategy than patching alone.

Skilled attackers are resourceful and, at times, utterly opportunistic. They can and will use any tool—any technique, any weakness, any piece of information—to build successful attack chains. Patches are not always effective, either, as evidenced by **CVE-2021-41773**, **CVE-2021-1732**, and Log4Shell CVE-2021-44228, all of which had at least part of their original fixes bypassed.

Additionally, many of the CVEs treated individually in this report can be used in concert with one or more additional vulnerabilities to achieve something beyond the scope of a single CVE's impact. Defenders can get ahead of future attacks by taking care not to treat individual vulnerabilities as if they existed in a vacuum, but instead choosing to implement controls and detection mechanisms across the whole of their environment.

At Rapid7, we believe that research-driven context on vulnerabilities and emergent threats is critical to building forward-looking security programs and advancing community knowledge. Security and IT teams face mounting challenges in a heightened threat climate, and we are committed to partnering with those teams to foster more in-depth understanding of defense-in-depth strategies that will strengthen organizations' security posture, both now and in the future.

For more information on the vulnerabilities featured in this report, and for Rapid7 and community analysis of new vulnerabilities and threats, keep an eye on **AttackerKB**.

For the full Rapid7 Vulnerability Intelligence Report click here