IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Reducing the Significant Risk of Known Exploited Vulnerabilities

November 3, 2021

OVERVIEW

The impact of cybersecurity intrusions that leverage vulnerabilities in information technology and operational technology products threaten the public sector, the private sector, and ultimately the American people's security and privacy. In 2020, industry partners identified a total of 18,358 new cybersecurity vulnerabilities, or Common Vulnerabilities and Exposures (CVEs). Of these, 10,342—an average of 28 per day—are classified "critical" or "high severity" vulnerabilities.

Organizations across both public and private sectors struggle to find time to test and implement remediations to these vulnerabilities—such as patches and updates—across complex infrastructures. Additionally, the effort and subject matter expertise required to research the degree of risk posed by a given vulnerability makes prioritizing CVEs a challenge.

In response to these challenges, the Cybersecurity and Infrastructure Security Agency (CISA), via Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, has created—and published on CISA.gov—a living catalog of known exploited vulnerabilities that carry significant risk. Approximately 200 vulnerabilities from 2017-2020 and 90 from 2021 make up the initial publication. CISA will regularly update the catalog with new known exploited vulnerabilities that meet specified thresholds.

CISA'S GOAL

The goal of BOD 22-01 is to enable federal agencies, as well as public and private sector organizations, to improve their vulnerability management practices and dramatically reduce their exposure to cyberattacks.

To accomplish this goal, all organizations should review and refresh their vulnerability management policies and playbooks, refer to the CISA catalog of known exploited vulnerabilities, and establish a more aggressive turnaround time to protect their networks against urgent, active threats.

CVE BACKGROUND

In 2015, CISA—then named the National Protection and Programs Directorate—determined the amount of time it took federal agencies to remediate the vulnerabilities that affected them—sometimes 200-300 days—was a significant risk. In response, CISA issued BOD 15-01 requiring federal agencies to fix or resolve known "critical risk" vulnerabilities detected on their systems within 30 days. Although agencies vastly improved in this area, four years later CISA found it necessary to issue another directive, BOD 19-02, requiring agencies to mitigate "critical risk" vulnerabilities within 15 days. BOD 19-02 also required agencies to resolve "high risk" vulnerabilities within 30 days.

The following items led to the issuance of BODs 15-01 and 19-02:

- CISA observed that cyber criminals and malicious actors were able to scan the internet for known vulnerabilities and exploit them within much smaller time frames;
- The total number of new vulnerabilities had skyrocketed from 2015 to 2018 from 6,487 to 17,305 ; 9,883 of these were rated "high" or "critical;" and
- The adaptability, sophistication, and speed at which cyber adversaries were targeting and exploiting known vulnerabilities outpaced agencies improved remediation time.

CURRENT THREAT

Currently, threat actors have launched increasingly damaging attacks against our nation's information systems, targeting

critical infrastructure such as water and oil suppliers, schools, and even hospitals. These attacks threaten our safety, our economy, and even our lives. Organizations are struggling to keep up with the increased sophistication and persistence of their cyber adversaries.

Over the last two years, CISA issued several Emergency Directives instructing federal agencies to focus their resources and efforts on remediating specific vulnerabilities and active exploits that CISA determined carried significant risk to the federal enterprise. A few recent examples include SolarWinds Orion code compromise, on-premises Microsoft Exchange, and Pulse Connect Secure.

CVE RISK SCORING

CISA has observed that risk scores, based on the Forum of Incident Response and Security Teams' Common Vulnerability Scoring System (CVSS), do not always accurately depict the danger or actual hazard that a CVE presents. Attackers do not rely only on "critical" vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated "high," "medium," or even "low."

In 2021, attackers chained four vulnerabilities, all subsequently rated as "high," to successfully exploit Microsoft Exchange servers. This methodology, known as "chaining," uses small vulnerabilities to first gain a foothold, then exploits additional vulnerabilities to escalate privilege on an incremental basis. CISA analyzes CVEs as they are disclosed to identify potentially chainable vulnerabilities and will push for them to be patched proactively, effectively preempting some of these attacks before they can be launched.

Also, many vulnerabilities classified as "critical" are highly complex and have never been seen exploited in the wild—in fact, only 4% of the total number of CVEs have been publicly exploited. But threat actors are extremely fast to exploit their vulnerabilities of choice: of those 4% known exploited CVEs, 42% are being used on day 0 of disclosure; 50% within 2 days; and 75% within 28 days. Meanwhile, the CVSS scores some of these as "medium" or even "low" severity.

CISA'S NEW STRATEGY

On November 3, 2021, CISA issued BOD 22-01, changing CISA's strategy of vulnerability management for federal agencies. Instead of only focusing on vulnerabilities that carry a specific CVSS score, CISA is targeting vulnerabilities for remediation that have known exploits and are being actively exploited by malicious cyber actors. Also, rather than issue individual Emergency Directives for each vulnerability of concern, BOD 22-01 institutes a mechanism that:

- Establishes a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise; and
- Requires federal civilian agencies to remediate these vulnerabilities within a more aggressive timeline.

BOD 22-01 drives federal agencies to mitigate the vulnerabilities on their networks that are most likely to result in a damaging intrusion, sends a clear message to all organizations across the country to focus remediation efforts on the subset of vulnerabilities that are causing harm now, and enables CISA to provide continuous prioritization of vulnerabilities based on our understanding of adversary activity.

For more information or to seek assistance, contact CISA at Central@cisa.gov.