4.6 Promote Deployment

Although we tend to think of the CVD process as ending with the disclosure of a vulnerability, if the fix is not deployed the rest of the exercise is futile. A patch that is quietly posted to a website and not well advertised is almost useless in protecting users from vulnerabilities.

Let's say that again, but clearer: **Vendors make patches *available*. But systems are not secure until those patches are *deployed*.**

Deploying patches typically implies provoking users, customers, and deployers to take positive action. Many software products are used by non-technical users. These users are often unaware of how to take remediative action for a vulnerability. A vendor's disclosure plan should consider how to reach the widest audience with actionable advice.

Products with secure automatic updates provide a good way to get a patch deployed quickly to a wide audience. However, not all users are able or willing to use automatic updates, so it is still important for vendors to draw attention to their fixes. Vendors should strive to implement easy and secure update methods in their products. In situations where this is not possible, the vendor's disclosure plan should be specific about how to spread the word of a new patch as quickly as possible.

Give Critical Infrastructure a Head Start When Possible

Some vulnerabilities are pervasive in the very infrastructure required for the patches or information about the vulnerability to be distributed. Vulnerabilities in foundational network protocols[1], or problems such as denial of service against backbone routers[2], remote code execution on Domain Name System (DNS) servers[3], or virtualization escapes[4] in cloud services serve as examples. Other vulnerabilities may disproportionately affect critical infrastructure services that directly impact public safety – for example the water system, power grid, or hospital medical gear. All these types of systems often require their operators to perform extra testing and impact analysis prior to deploying patches. It's not always practical to do so, but when possible, providing these kinds of deployers with advance notification of either the existence of the vulnerability or access to the fix can reduce the risk faced by the public and improve outcomes.

Amplify the Message

Sometimes it is necessary to draw more attention to a problem or fix. Critical vulnerabilities, including those that are already being exploited or are highly likely to be exploited, may warrant attracting attention beyond merely publishing a document on the vendor's support site. In such cases, additional measures should be taken to draw attention to the existence of the vulnerability or the availability of its fix. (See also 4.5 Gaining Public Awareness)

Vendors should consider using:

- Announcements via social media. Many defenders use services like Twitter or Reddit as part of their daily situation awareness process, routinely sharing useful links and references with each other.
- Mass media such as press releases, press conferences, and media interviews
- Working with a coordinator or government agency to draw attention to a vulnerability or its fix. In particular, National CSIRTs can often provide advice or assistance with publicity on important issues.

Post-Publication Monitoring

Once a vulnerability and/or its fix has been disclosed, both vendors and reporters should look for feedback concerning any problems with either the documentation or the fix. In some cases, this can take the form of technical monitoring (e.g., monitoring download logs from the vendor's update service, checking inventories of deployed system versions, or even scanning) to ascertain the rate

CVD Goes to Washington

In an unexpected turn of events following the publication of this Guide, we were called on by the US House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation to address concerns regarding the coordinated disclosure of the Meltdown and Spectre vulnerabilities in early 2018. In particular, the committees were concerned about the timing of patch availability and deployment relative to the public disclosure of these vulnerabilities.

> *In their responses to the Committees' letters, many of the companies explained that it is industry best practice to embargo vulnerability information amongst the smallest possible group of stakeholders during CVDs to prevent "bad actors" from learning of the vulnerability or vulnerabilities before they have been corrected. Many of the companies further advised that they followed or otherwise cited the CVD protocol or guidance provided by the CERT Coordination Center (CERT/CC). In addition, many respondents further argued that it is critical to do so to ensure that patches are "in place," "delivered," or "implemented" prior to widespread public disclosure. As a company or user is not protected from a given vulnerability until an appropriate patch is "in place," "delivered," or "implemented," we agree that sound CVD strategies would seek to limit disclosure of vulnerability information before stakeholders are able to apply patches. Such a practice allows for the best protection of the end user–typically, consumers.*

The committees went on to note:

of defender deployments. Even if such technical monitoring is not possible, not permitted, risky, costly, or otherwise impractical, it is usually possible to monitor for user feedback via support requests, online discussions, and so forth.

In the event of slow uptake of the fix, additional effort might be warranted to call attention the vulnerability (for example, using social media).

It is also possible that the remediation advice is incorrect, or may not apply to all scenarios. Therefore the vendor and reporter should monitor for public discussion or reports of problems, so that the disclosure advisory and remediation information can be updated as necessary. Remember, the goal for remediation is to fix vulnerable product instances or at least reduce the impact of the vulnerability. Consequently, if a significant portion of the vulnerable product instances have not been remediated, that goal has not been achieved.

References

1. Havrilla, Jeffrey. "Multiple TCP/IP implementations may use statistically predictable initial sequence numbers Vulnerability Note VU#498440." 13 March 2001. https://www.kb.cert.org/vuls/id/498440/
2. Juniper. "2018-10 Security Bulletin: Junos OS: Receipt of a specifically crafted malicious MPLS packet leads to a Junos kernel crash (CVE-2018-0049)." 10 October 2018. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10883&cat=SIRT_1&actp=LIST
3. Cohen, Cory. "ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code Vulnerability Note VU#196945." 29 January 2001. https://www.kb.cert.org/vuls/id/196945/
4. XEN. "Xen Security Advisory CVE-2017-8903 / XSA-213; version 3; x86: 64bit PV guest breakout via pagetable use-after-mode-change." 2 May 2017. https://xenbits.xen.org/xsa/advisory-213.html

> *However, based on the responses to our letters and information provided during company briefings, questions remain regarding...whether companies used precise terminology in describing the* availability, *not* appli cation*, of patches. Companies outside the core group needed time to test and successfully implement patches, and the availability of a patch and the application of a patch are not the same. The fact that a patch or other mitigation is "available" simply means that it exists and is ready for a company or individual to use. But when a patch or other mitigation is described as "in place," "delivered," or "implemented," the distinction implies that companies and individuals have retrieved that patch and actually applied it to their systems.*

In our response, we agreed. The relevant section of our reply is reproduced below.

Patch Availability is not Patch Deployment

The committees' letter asks "...whether companies used precise terminology in describing the availability, not application, of patches" and points out "...the misapplication of such terms as 'in place' and 'available' when used to describe the status of vulnerability patches."

CVD guidance can be more clear in both terminology and the boundary between the phases of patch availability and patch deployment. And while we agree that vendors should take care not to overstate the status of patch deployment, the best many vendors can do today is to make patches available, along with sufficient vulnerability information for users to make informed patching and other risk decisions.[1] Ultimate responsibility for installing patches often falls to deployers,[2] including end users.

While we appreciate the committees' desire that "sound CVD strategies would seek to limit disclosure of vulnerability information before stakeholders are able to apply patches," our experience indicates that it is impractical to privately notify all affected stakeholders without public disclosure. Thus, public disclosure is usually the best practice to inform affected parties—including end users—who may need to take action in order to apply patches to their software and devices.

The committees' letter correctly points out that the deployers' need to test patches "can lead to a lag time of weeks or months before a patch is applied." We note that in the extreme, this lag time can become indefinite for reasons including:

- Some deployers (including many end users) will remain unaware of the availability of patches, or will lack the technical capability to deploy them successfully.
- Long or complex supply chains for patch distribution may result in patches issued by an originating vendor not making it through to the downstream vendors' products in a timely manner.
- Some deployers will intentionally choose to accept the risk and not apply the patch at all. The decision to apply patches is a risk management decision.

For especially pervasive vulnerabilities such as Meltdown and Spectre, there is no clear optimal solution to balancing the diverse operational cadence across such a wide range of industries (including critical infrastructure sectors) with the need for timely public disclosure. It may be that the best we can expect is for consistent, accurate, thorough, and timely information to be provided in support of defender decisions.

---

1. Some products have secure, robust, and automated patch deployment features. Software-as-a-service (SaaS) and other cloud services can typically be updated by providers, requiring little if any action by end users.
2. By "deployers" we mean those responsible for choosing if, when, and how to install patches or perform other mitigating or compensating actions. Deployers can include system administrators, vulnerability management systems, vendors with the ability to push patches, and end users who must take manual action.