IMPROVING VULNERABILITY DISCLOSURE TOGETHER

November 27, 2019
8:32 am

By Jeanette Manfra, Wednesday November 27th, 2019

At CISA, we work to do good things. Some are easy, like eating pineapple on pizza. Some are hard, like managing risks in 5G. Yet we know that if it's hard to do good things, most people won't do them – and reporting a vulnerability on a government system shouldn't be so hard.

A VDP directive and you

Today, **we are issuing a draft binding operational directive**, BOD 20-01, which will require federal civilian executive branch agencies to publish a vulnerability disclosure policy (VDP). A VDP allows people who have "seen something" to "say something" to those who can fix it. It makes clear that an agency welcomes and authorizes good faith security research on specific, internet-accessible systems.

In preparing this directive, we've worked with several agencies that have VDPs and made an effort to align the directive with federal guidance, international standards, and good practices. But this directive is slightly different from others we've issued, where agencies are directed to take an action and then CISA verifies the action has taken place. Here, while agencies must maintain VDPs and are the beneficiaries of vulnerability reports, it's the public that will provide those reports and will be the true beneficiaries of vulnerability remediation. That's why we're doing something we've never done before with our directives: **seeking public feedback before issuance**.

We want to hear from people with personal or institutional expertise in vulnerability disclosure. We also want to hear from organizations that have a VDP and manage coordinated vulnerability disclosures.

In seeking public comment, we're also nodding to the fact that, to our knowledge, a requirement for individual enterprises to maintain a vulnerability disclosure policy has never been done before, and certainly not on this scale.

Do's and don'ts

What's the draft directive do?

- **Lights a fire**. Each agency must publish a VDP and maintain handling procedures, and the directive outlines a set of required elements for both.

- **Draws a line in the sand**. Systems "born" after publication of a VDP must be included in scope of an agency's VDP.
- **Expands the circle**. Until everything is included, at least one new system or service must be added every 90 days to the scope of an agency's VDP.
- **Starts the clock**. There's an upper bound – 2 years from issuance, in this draft – for when all internet-accessible systems must be in scope.
- **All are welcome**. Anyone that finds a problem must be able to report it to an agency.
- **No "catch and keep"**. An agency may only request a reasonably time-limited restriction against outside disclosure to comply with their VDP.
- **Defense, not offense**. Submissions are for defensive purposes; they don't go to the Vulnerabilities Equities Process.

What doesn't it do?

- **Does not establish a "federal bug bounty"**. A bug bounty is a program that pays researchers for valid and impactful findings. Nothing in the directive prevents individual agencies from establishing a bug bounty of their own, though.
- **Does not create a "national VDP"**. The directive is an executive branch policy instruction that requires federal civilian executive branch agencies to have a VDP. The difference might appear slight but they're very different things.

Why isn't this a national VDP? We think a single, universal vulnerability disclosure policy for the executive branch is a good goal. It makes sense particularly when each agency has all internet-accessible systems in scope, but we expect that goal to be an unrealistic starting place for most agencies. Instead, the directive supports a phased approach to widening scope, allowing each enterprise – comprised of the humans and their organizational tools, norms, and culture – to level up incrementally.

Doing good things together

We believe that if you make good things easier to do, more people will do them. With this directive, we want to take steps that diminish complexity and make expectations plain. In support of that, we're also sharing draft implementation guidance on the directive, as well as a draft VDP template.

We welcome your feedback and perspective on all these documents, as well as any comments on our approach. The public comment will take place on GitHub and last until December 27th, 11:59pm EST.

Taxonomy Topics: Cybersecurity

Keywords: CISA, vulnerability

REPORT