Zero Day Broker SSD Sells Early Access To Cybersecurity Vulnerabilities

Published on Aug 17, 2023

Charles Rollet

While the norm for cybersecurity disclosure is to share vulnerabilities only with the vendor until the vendor fixes them, zero-day broker SSD has built a business selling early access to vulnerabilities across a broad range of applications from OSes, to web browsers, mobile and IoT devices.

SSD told IPVM they follow responsible disclosure and vet who they sell this early access to.

This atypical model, generally offering far greater payments, challenges vendor bug bounty programs and many vendors' expectations that researchers will simply inform them at no charge.

However, this also raises concerns about which buyers are obtaining early

access and what they will do with that.

SSD Background

SSD Secure Disclosure pays security researchers to uncover vulnerabilities for "a vast scale of software and hardware". SSD is registered in Israel with entities in Seoul, Tokyo, and Hanoi (via SSD Labs) and holds an annual conference in Seoul called TyphoonCon.

In June 2023, IPVM examined SSD offering up to $75,000 for Uniview vulnerabilities, in contrast to Axis' bug bounty program only offering up to $3,000 rewards (which Axis later doubled to $6,000.)

SSD: Customers Pay For "Early Heads-Up"

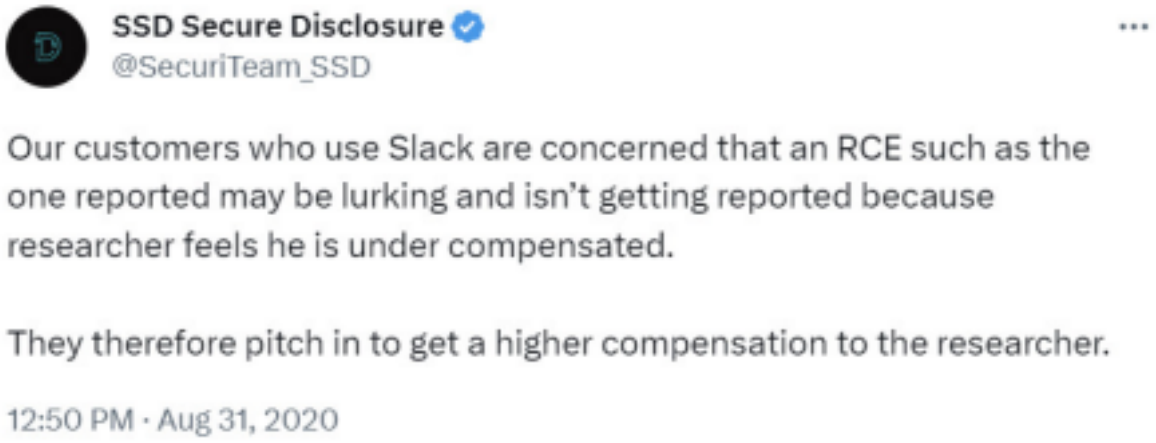
SSD is currently seeking vulnerabilities for Axis and Mobotix, but both firms told IPVM they are not working with SSD, raising the question of who pays SSD if not the vendors.

SSD told IPVM it is paid by a combination of vendors and customers who "want an early heads-up on possible vulnerabilities in the devices they are using":

> SSD works with security researchers who enjoy hunting for security vulnerabilities and like the option of getting paid for their time and effort. All vulnerabilities are disclosed to the vendor for fixing and the disclosure timeline is coordinated with the vendor.
> Payment comes from the vendors in the form of bounty for vulnerabilities found and from **customers of those vendors who want an early heads-up on possible vulnerabilities in the devices they are using.**
>
> We can't comment on our work with specific vendors or customers, and we will also not comment on other disclosure programs' policies or methods. We are proud of our contribution to the security research world over the last several decades and we believe that the growth of the ecosystem is a good thing for everyone. If anything, we'd like

> to see more bounty programs, more disclosure companies, and much more security research being done. We're happy that things are trending in the right direction.
>
> We do realize that in the short term having researchers disclose security vulnerabilities is irritating to the device manufacturer, but in the long term it makes the devices more secure, and by extension our own networks more secure. It's a huge net gain for the digital society.
>
> SSD plans to continue helping researchers, vendors and customers to further secure our digital world. [emphasis added]

This echoes a 2020 SSD tweet that some of its customers pay to find vulnerabilities in the products they use (Slack, in this case) as the vulns would otherwise not be reported "because researcher feels he is under compensated".



SSD Says Vulnerability Usage "Ethical And Lawful"

IPVM asked SSD twice if it permits its customers to use this "early heads-up" for hacking/offensive purposes.

SSD did not directly respond, instead stating all its customers go through due diligence and their usage is "ethical and lawful":

> As mentioned, **all our customers go through due diligence** and we

> verify that their usage of the information is **ethical and lawful.** There are no exceptions. Also, as mentioned, **all vulnerabilities are reported to the vendor**, and there are no exceptions here either. [emphasis added]

Using vulnerabilities for hacking purposes has been justified as being in an "ethical and lawful" manner, e.g., the FBI hacking terrorists though whether and when this is "ethical and lawful" is debated.

SSD "Supports and Encourages Responsible Disclosure" SSD

told IPVM it "supports and encourages responsible disclosure":

> SSD Disclosure **supports and encourages responsible disclosure**. The founders of SSD Disclosure were the founders of a security portal called SecuriTeam.com, back in 1998, which was one of the first full-disclosure web sites. We've defended researchers against SLAPP lawsuits and helped researchers conduct security research without fearing retaliation.
>
> To this day we still assist researchers, free of charge, in all matters relating to responsible disclosure. SSD is a direct extension of that effort - for researchers who want to get paid for findings. The two are not mutually exclusive. [emphasis added]

SSD also says it has been "Disclosing vulnerabilities responsibly since 2007" on its LinkedIn page.

Responsible Disclosure To Only Vendors The Norm

However, the accepted ethical norm is responsibly disclosing just to vendors i.e. not re-selling to others. For example, the Zero Day Initiative - the largest zero day broker by total disclosures - explicitly states "we do not resell or redistribute the vulnerabilities that are acquired through the ZDI."

Closer to SSD's model is Zerodium, which re-sells vulnerabilities to its customers while similarly stressing, "We take ethics very seriously and we choose our customers very carefully through a very strict due diligence and vetting process."

However, Zerodium does not publicly say it supports responsible disclosure nor reports vulnerabilities to vendors, as SSD does. SSD also publishes advisories/disclosures of its findings, unlike Zerodium.

SSD told IPVM, "We can't comment on our work with specific vendors or customers, and we will also not comment on other disclosure programs' policies or methods."

SSD Co-Owner Unit 8200 Graduate

Noam Rathaus is "Managing the SSD Secure Disclosure program" per Israel's official startup portal; Rathaus is also listed as co-owner of SSD by Israel's corporate registry.

Rathaus is a former member of the Israeli military intelligence's cyber division, Unit 8200, according to a 2002 article from the Israeli newspaper Haaretz. Unit 8200 is roughly equivalent to the NSA in the US and "specializes in sophisticated hacking and espionage operations," Motherboard reported.

Risks Examined

It is possible that SSD's customers only seek an "early heads-up" to protect the devices they are using. However, SSD did not entirely rule out these vulnerabilities being used offensively, either.

Large manufacturers often pay relatively low bug bounties (or none at all), e.g., Axis offering up to $6,000 per bounty. giving significant incentive to researchers - who may spend hundreds of hours finding a single exploit - to sell to SSD or others.

Vendors (and their end users) listed in SSD's 'Scope' should thus be aware that SSD may be sharing early access to their vulnerabilities, giving them reason for caution.