The Linux kernel is a key component for the security of the Internet. Google uses Linux in almost everything, from the computers our employees use, to the products people around the world use daily like Chromebooks, Android on phones, cars, and TVs, and workloads on Google Cloud. Because of this, we have heavily invested in Linux's security - and today, we're announcing how we're building on those investments and increasing our rewards.

In 2020, we launched an open-source Kubernetes-based Capture-the-Flag (CTF) project called, kCTF. The kCTF Vulnerability Rewards Program (VRP) lets researchers connect to our Google Kubernetes Engine (GKE) instances, and if they can hack it, they get a flag, and are potentially rewarded. All of GKE and its dependencies are in scope, but every flag caught so far has been a container breakout through a Linux kernel vulnerability. We've learned that finding and exploiting heap memory corruption vulnerabilities in the Linux kernel could be made a lot harder. Unfortunately, security mitigations are often hard to quantify, however, we think we've found a way to do so concretely going forward.

Simply finding vulnerabilities and patching them "is totally useless," according to Google's Eduardo Vela, who heads the cloud giant's product security response team.

"We don't care about vulnerabilities; we care about exploits," he told The Register in an exclusive interview. "We expect the vulnerabilities are there, they will get patched, and that's nice and all. But the whole idea is what do to beyond just patching a couple of vulnerabilities."
To this end, Google's open-source, Kubernetes-based Capture-the-Flag (kCTF) project doesn't pay researchers a bounty to just find a Linux Kernel vulnerability. Instead, they've got to exploit the bug: connect to Google Kubernetes Engine (GKE) instances, hack it, and use the bug to steal the hidden flags.

Google's New Bug Bounties Include Their Custom Linux Kernel's Experimental Security Mitigations - Slashdot [4]

Google uses Linux "in almost everything," according to the leader of Google's "product security response" team ? including Chromebooks, Android smartphones, and even Google Cloud.

Sending Spammers to Password Purgatory with Microsoft Power Automate and Cloudflare Workers KV [5]

How best to punish spammers? I give this topic a lot of thought because I spend a lot of time sifting through the endless rubbish they send me. And that's when it dawned on me: the punishment should fit the crime - robbing me of my time - which means that I, in turn, need to rob them of their time. With the smallest possible overhead on my time, of course. So, earlier this year I created Password Purgatory with the singular goal of putting spammers through the hellscape that is attempting to satisfy really nasty password complexity criteria. And I mean really nasty criteria, like much worse than you've ever seen before. I opened-sourced it, took a bunch of PRs, built out the API to present increasingly inane password complexity criteria then left it at that. Until now because finally, it's live, working and devilishly beautiful

Security

Source URL: http://www.tuxmachines.org/node/168308

Links: