CVE Program FAQ

What is Red Hat's contribution to the CVE Program?

Red Hat has been a CVE Program partner since 2002, as a CNA. Red Hatters are passionate and actively involved in various special working groups in the MITRE CVE Program. In September 2022, in recognition of Red Hat's reputation and support to the open source community in the CNA Program, the CVE Program designated Red Hat as a Root organization for open source organizations and projects. The CVE Program has matured, expanded, and continues to grow, and we are proud to say that Red Hat is a major contributor to the CVE Program's success. One example worth mentioning is the popular "cvelib" Python library and command line interface for the CVE Services API, which is developed and maintained by Red Hatters.

What does Red Hat do as a Root?

As a Root CNA, Red Hat is responsible for mentoring and assisting CNAs that have chosen us as their Root. We encourage, contribute, and support the open source projects in the Program to be successful. We operate beyond our organization's scope and go the extra mile to support our CNAs. We also help the CVE Program with its expansion and share the workload with other Root CNAs and the Program Secretariat.

For more information, visit our blog, How Red Hat supports open source vulnerabilities within the CVE Program.

What information will Red Hat have access to, for their CNA's?

For vulnerabilities with assigned CVEs, Red Hat will have similar access to other CNAs in the program. For example, if you have any embargoed CVEs, Red Hat will not have access to that vulnerability information unless and until you publish that CVE record.

Having said that, as a Root, we have access to your preliminary information, such as the point of contact submitted during CVE Program registration. If a dispute or conflict arises from a CVE that you have assigned, or if another CNA assigns a CVE for a vulnerability in your scope, Red Hat can step in to help conclude the situation within the CVE Program's policy.

Why should we choose Red Hat as our Root?

Red Hat is the largest open source company in the world. We build and support open source products from community projects, giving back to the community and defending open source every step of the way. We have a strong rapport and connections with many upstream

communities, and many Red Hatters are maintainers in upstream open source projects. As a Root CNA, we go above and beyond to help our CNA's in every possible way, whether it's technical assistance, automation, governance, or collaboration with other open source projects and upstream communities at large. Red Hat has been a CVE program partner since 2002, and our experience has taught us the value of being involved and engaged with the CNA community to improve data quality and drive standards adoption. We are on the CVE board and are actively involved with industry coordination working groups and MITRE SIGs, contributing to strategic planning, CVE automation, CNA coordination, CWE, and CVE quality working groups. We also have a world class Product Security Incident Response Team (PSIRT) with matured and proven processes, tooling, and workflows. We are always willing to share our experience and knowledge with open source projects to mature incident response processes.

Like many CNAs, we have developed many of our own tools to manage CNA tasks and vulnerability analysis. We would be happy to help mentor and collaborate on the tools we've developed around CVE services and with the tools we use for flaw analysis and vulnerability management

For more information, visit our blog, Our CVE story: Why Red Hat became a Root.

I want to choose Red Hat as our Root. How do I start?

Send us an email at rootcna-coordination@redhat.com. One of our Product Security specialists will reach out and guide you through the process.