How do I report a security vulnerability to Cyber Crucible?

Short answer: Email **security@cybercrucible.com**. Describe the issue, the product and version affected, and the steps to reproduce it. We confirm we have your report, keep you updated while we investigate and, where needed, fix it, and agree with you on when the issue can be made public. Security research carried out in good faith and in line with this policy is welcome.

What is in scope

- **Cyber Crucible Core**, the endpoint agent for Windows, Linux and macOS, including its kernel drivers, services and installers.
- **FortressAI**, the generative-AI data protection agent for Windows.
- **The Cyber Crucible Platform** management service: the dashboard web application, the REST API, and the agent tasking and authorization services.
- **Sites Cyber Crucible operates:** www.cybercrucible.com, knowledgebase.cybercrucible.com and dashboard.cybercrucible.com.

What is out of scope

- Services run by third parties, even where Cyber Crucible uses them. Report those to the provider.
- Denial-of-service testing, load testing, and anything that degrades a service for other users.
- Social engineering, phishing, or physical attempts against Cyber Crucible staff, offices or partners.
- Findings from automated scanners with no demonstrated security impact, missing best-practice headers on their own, and self-XSS.
- Weaknesses in a customer's own environment or configuration. Please tell the customer directly.

What to include in your report

- The product or site and the version, build or URL affected.
- A clear description of the issue and its security impact.

- Step-by-step instructions to reproduce it, with a proof of concept where you have one.
- Whether it's being exploited, as far as you know, and whether you've told anyone else.
- How you'd like to be credited, or whether you'd rather stay anonymous.

Sending sensitive details

Send everything to **security@cybercrucible.com**, including exploit code or a proof of concept. The mailbox is monitored, and no form or encryption key is needed. If you came across credentials, don't send them: tell us where you found them, and we'll rotate them. Don't include anyone's personal data unless it's essential to show the issue.

What happens after you report

1. **Acknowledgement.** We confirm that we've received your report.
2. **Assessment.** We reproduce the issue, assess its severity and exploitability, and may come back to you with questions.
3. **Fix.** Fixes go through our patch-management and change-management process. Issues that are being actively exploited take an expedited path. Windows kernel-driver updates are submitted to Microsoft's Windows Hardware Compatibility Program before release.
4. **Updates.** We tell you when the fix is ready, and agree with you when the issue can be disclosed.

Coordinated disclosure

Please give us a reasonable chance to fix the issue before you make it public, and talk to us about the timing. We'll keep you informed, and we'll credit you in the release notes when the issue is disclosed, unless you'd rather we didn't.

Good-faith research (safe harbor)

If you research and report a vulnerability in good faith, following this policy, we'll treat your work as authorized and won't pursue legal action against you for it. Good faith means you:

- test only against accounts, groups and devices you own or have permission to test, and never against another customer's group or data;
- only access, change or keep the data you need to show the issue, and stop and tell us as soon as you reach anyone else's data;
- delete any data you obtained once the report is closed;
- don't degrade, disrupt or damage our services or other users;

- don't use the issue for anything beyond showing that it exists;
- give us a reasonable time to fix it before disclosing it;
- follow the law that applies to you.

We can only authorize research against systems Cyber Crucible controls. This policy doesn't bind our customers or our service providers, and it doesn't authorize reverse engineering, decompiling or disassembling Cyber Crucible software beyond what your license allows.

If you're unsure whether something is allowed, ask us at security@cybercrucible.com first.

How security fixes are published

Security updates and bug fixes ship in Cyber Crucible software releases and are documented in the release notes in Software Releases. Agents on auto-update download a fix automatically, and it takes effect at the next reboot. Where auto-update is off, an administrator approves the version first.

Related

- Does Cyber Crucible have a patch management program?
- Does Cyber Crucible have an incident response and breach-notification process?
- Where can I find Cyber Crucible's security, compliance, and trust documentation?

Revision #1
Created 2026-11-24 04:48:53 UTC by Dennis Underwood
Updated 2026-11-24 04:48:53 UTC by Dennis Underwood