[NEW] Security Advisories

ONE OF OUR CORE VALUES IS TO BE TRANSPARENT IN OUR ACTIONS ACROSS THE ORGANIZATION

Here at Devolutions, one of our core values is to be transparent in our actions across the organization. As part of this commitment, today I am pleased to announce that **going forward, we will be publishing Security Advisories when vulnerabilities are discovered and fixed in all of our products.**

About Security Advisories

Security Advisories provide information about **newly discovered software vulnerabilities**, and include details such as the **type of vulnerability, severity, affected versions, fixes, and potential workarounds**. The practice of sharing this information has been adopted by major software vendors and is crucial for helping network administrators and security teams determine their level of exposure and prioritize updates.

Naturally, it is best to patch early and often. However, upgrades come with their own set of challenges. Having specific information about vulnerabilities makes it possible to better assess risks to an organization and decide how quickly they should be addressed.

Each vulnerability is also given a Common Vulnerabilities and Exposures (CVE) number that uniquely identifies it. CVEs are assigned by the MITRE and can be searched in public databases such as the NVD. They are also used in various tools, such as inventory management systems and security scanners, which make it easier for organizations to identify their vulnerable assets.

From the desk of our CSO Martin Lemay:

Having the capacity to publish security advisories is not as easy as most people tend to believe. It requires the involvement of multiple processes and people to synchronize publications with software releases. Key tasks include:

- *Reported vulnerabilities need to be reliably fixed on all supported versions.*
- *CVEs must be documented and reserved prior to the release date.*
- *The advisories must be documented to reveal enough information about security issues, but without putting customers at unnecessary risk.*
- *The website must be updated and accessible at the exact time of the release.*

If for some reason the release date is postponed, then everything must stay synchronized to the new date! All this, of course, must occur without impacting business velocity.

I am extremely proud to work for a company that is committed to moving ahead with this kind of major security initiative, demonstrating transparency and honesty in all practices. Yes, mistakes can happen. But at Devolutions we are focused on fixing them rapidly, and informing customers about these issues and resolutions. As Simon Sinek has famously said: "Trust is built on telling the truth, not telling people what they want to hear."

This initiative will be constantly monitored for improvement from now on. We also have more transparency-oriented projects in the pipeline coming out soon. Stay tuned!

Report a Security Issue

If you have any questions about our Security Advisories or any other aspect of our security program, then **please contact us at security@devolutions.net**.

We also invite you to contact us to report a security issue, and we thank you in advance for helping us ensure that our products continuously achieve the highest data security standards.