CVE to Ivanti Patch Solution

This architectural solution overview does not constitute a formal offer of product.

Executive Summary

Ivanti's CVE-to-Patch solution provides a critical missing link in security best practices for patching in the corporate ecosphere—whether in cloud-based computing, endpoint, or customer-premises IT infrastructure. It helps Security Operations (Sec-Ops) teams identify, address, and remediate vulnerable software and systems based on the full CVE (Common Vulnerabilities and Exposures) listings found in security scan reports. But most importantly, it provides the opportunity to automate this process shared by IT and Sec-Ops teams.

This unification minimizes exposure to breaches that occur commonly between IT and Sec-Ops teams. Such breaches, if left unaddressed, can lead to confidential data loss, loss of internal system controls, and other unanticipated negative results. Mitigating security risk begins with healthy patching hygiene—and through Ivanti, automating CVE to Patch is an achievable element of this best practice.

Why Ivanti – Key Use Cases

Ivanti provides our customers with a cloud-based RESTful API that enables security engineers, security products and platforms, security orchestration and automation tools, and threat intelligence platforms to query a definitive list of remediations for a given vulnerability. Submitting one or more vulnerabilities in the form of CVE numbers, gathered either through manual research or as result of using security tools like security scanners, allows the API to retrieve associated remediations.

We have the largest collection of patch content for OS platforms like such as Windows and Red Hat Enterprise Linux, and for third-party applications like Adobe, Firefox, etc. We are in process of adding support for CentOS, macOS, and Ubuntu as well. While vendors are quick to release patches for a given vulnerability, they sometimes update, or even withdraw and publish, new patches for the same vulnerability. We have a dedicated team of engineers who monitor and maintain the latest list of remediations for given vulnerabilities.

Case Enrichment

Incident response teams and/or Security Orchestration and Automation tools can access the API to enrich a specific case with critical actionable information, including:

- List of remedies
- Products affected by the patch and associated OS information
- Release date
- Vendor severity
- Detailed description and link to vendor-published information
- Superseded patch information
- Additional CVEs mitigated by the patch

Compliance Enforcement and Reporting

Sec-Ops teams can maintain a baseline list of CVEs that must be remediated in their environment. They can then correlate patch information from our API with the patch management tools in their environment to establish compliance and produce more accurate security-risk reports. With the help of automation tools, it is easier to enforce compliance in real time.

Unified IT and Remediation

- **Service Management platforms:**
  With the information from our API, Sec-Ops teams can create a support ticket from a variety of service management platforms and send the list of patches that must be remediated by IT-Ops teams.
- **Patch Management platforms:**
  With the information from our API, Sec-Ops teams can create a patch task on Patch Management platforms like Ivanti Security Controls or Windows Update and trigger the process of patching.
- **Security Automation and Orchestration platforms:**
  Sec-Ops can automate Security Processes with the information provided by the API.
- **Through your product:**
  You can also integrate your product with our Patch SDK to fully integrate the patching of endpoints.

Conclusion

Implementing Ivanti CVE-to-Patch API based on Common Vulnerability Exposures make it possible for organizations to bridge common organizational gaps between IT Security and IT Operations by delivering accurate patch assessment for security purposes, and packaged security patches and tools for operations to perform remediation.

About Ivanti

LANDESK and HEAT Software combined in January of 2017 to form Ivanti. Click to read the history, including the stories of Shavlik, AppSense, Xtraction Solutions, RES, and others, or for more information, visit www.ivanti.com.

Our mission is clear—to help customers succeed in their respective markets through the "Power of Unified IT".

Learn More

ivanti.com
1 800 982 2130
sales@ivanti.com