ivanti

SOLUTION SHEET

# Risk-Based CVE to Patch Approval

## Now Available in Ivanti Patch Management Solutions

**Ivanti provides the ability to read-in vulnerability scan results, view the identified Common Vulnerabilities and Exposures (CVEs) and associated patches, and publish or approve any missing patches for deployment.**

Chances are your IT Operations team and your IT Security team "speak different languages." The Ops team needs things to run smoothly, while the Security team must safeguard the environment. Yet both teams share a common goal—to secure and enable the business. And it's at the endpoint where they must work together to achieve it.

### Continuous Vulnerability Assessment and Remediation

It's true that continuous vulnerability assessment and remediation should be part of every organization's security practices, yet the time and manual work involved from when a vulnerability is first identified to when a software update is deployed is taxing.

While one vulnerability is easy to identify and remediate, you've likely seen a vulnerability report from the Security team detecting at least 1,000 CVEs. But what if it's 10,000 or even 50,000 CVEs? A single vulnerability assessment may find multiple problems on systems throughout your environment—and the same vulnerabilities can appear on many different systems and in many pieces of software on the same system.

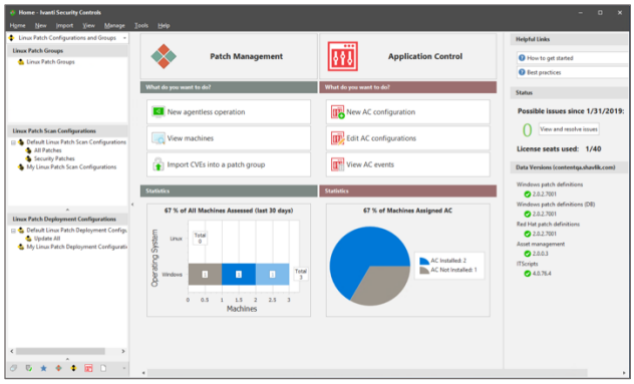
Very quickly the assessment and remediation effort becomes a complex, full-time job. And attackers can leverage that time to gain a foothold to access sensitive data. The longer it takes to sort and plan, the more susceptible you are to security incidents. IT Ops must pore through the reports from the Security team, identify CVEs, match them up against a given update, and then push them out through your patch management solution.

### Reduce the Time from CVE to Patch

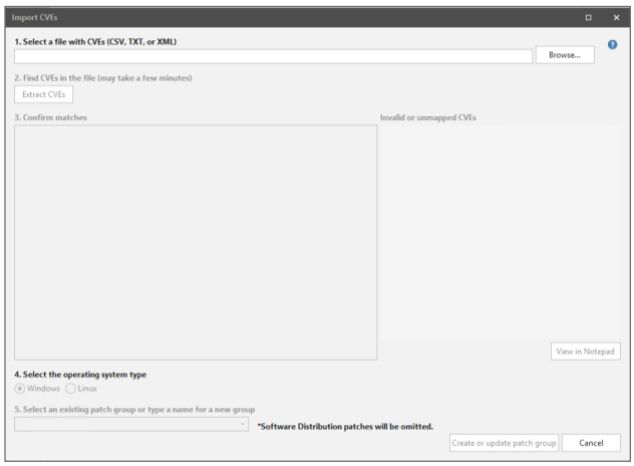
Thanks to the CVE-to-patch import capability in Ivanti solutions, you can streamline the process from hours to minutes. Whether you're using vulnerability assessments from Rapid 7, Tenable, Qualys, BeyondTrust, or another vendor, Ivanti solutions map the patches that relate to those CVEs and build a patch list of updates that you can quickly approve or publish for remediation in your environment.

### Let's Take a Closer Look

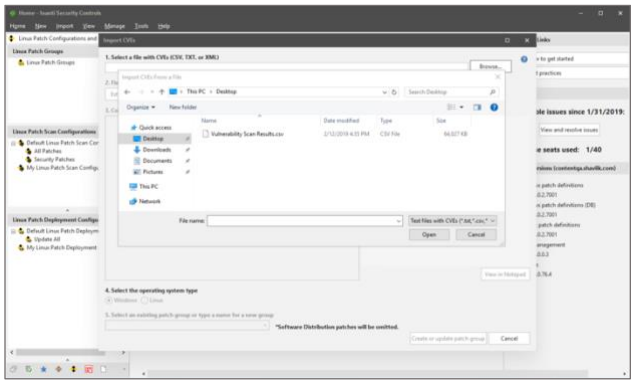
This screen shot shows the new Ivanti® Security Controls home screen where you can select "Import CVEs into a Patch Group."



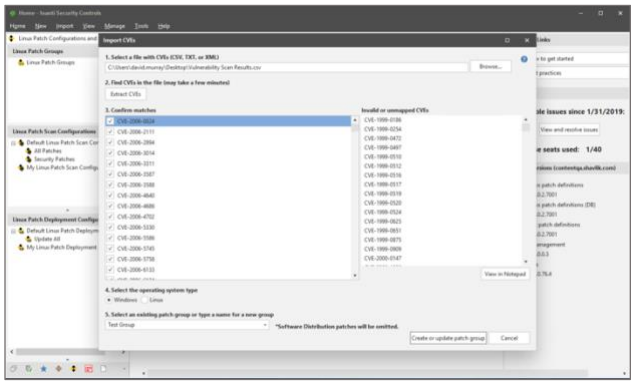
Whether you have XML files, CSV files from spreadsheets or databases, or plain-text files that you've created that identify CVE information, they can be used in conjunction with this import feature. Ivanti's patch solutions are able to scrape through the information and map the CVEs to the software updates you need to resolve the vulnerabilities.




As shown in this next screen shot, we're going to read in the CVE information from a 64MB file:



Next, we can identify the CVEs, match them with the updates that address these particular vulnerabilities, and show you exactly what patches you would need to apply on your endpoints:



In the example above, there were 4,880 CVE IDs. Without this Ivanti technology, manually identifying the 1,369 associated updates that address these vulnerabilities would take hours to days to research each time the Security Team provides a new report to Operations.

**For more information on these capabilities available in Ivanti patch management solutions, please contact sales@ivanti.com.**

## Learn More

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