Address Detected Vulnerabilities More Quickly

**Now you can:**

- Act quicker by leveraging a comprehensive repository of third-party patch data
- Discover which vulnerabilities in your unpatched products have the highest risk of exploitation
- Save time creating patches to update software in your environment

**What you get**

The amount of exploits, attacks and other vulnerabilities that come up daily can be overwhelming. Flexera Software Vulnerability Manager (SVM) does a great job of exposing them, and then helping to prioritize remediation efforts. With the new Vendor Patch Module, you can take advantage of these insights and deal with them quickly using the most comprehensive patch coverage on the market — with more than 1000 out-of-the-box patches. Plus, the Vendor Patch Module delivers details to help you more easily create over 1000 additional patches.

**Leave third-party patch catalogs behind**

One increasingly popular way to address the need for patches is to subscribe to third-party patch catalogs. However, those are just blind sets of patches which may overlap with some percentage of the applications that are important to your organization. While it may save you some work, you can only measure your success against the deployment of the provided patches.

A better approach to vulnerability management is to know what software you have, what’s vulnerable and how serious a threat it represents to your organization. SVM gives you this valuable insight, and with the new Vendor Patch Module, you can take action quickly by leveraging our exhaustive repository of third-party patch data.

**Choose an integrated approach**

We offer an integrated solution providing you the best third-party software coverage on the market today. Leveraging research conducted by Flexera’s Secunia Research team, you can effectively locate, prioritize threats and remediate them quickly to lower the risk to your organization. With hundreds of software vendors and thousands of software titles, it’s difficult to know what patches are even available, or what patches represent a security risk if you were to delay patching. By combining all these capabilities in a single solution, you’re able to effectively manage your security risk—all the way from initial visibility, to knowing which patches should be handled first, to getting armed with those patches.
Make prioritization a priority

While the Vendor Patch Module makes it much easier to publish patches, each requires testing and introduces some level of risk if such a deployment negatively impacts endpoints. That’s why effective prioritization is so important. Flexera offers the ability to prioritize based on the criticality or CVSS score from the vulnerability research we provide, by how many instances are detected in your environment and by Active Directory group to help you focus on more critical devices as necessary.

Prioritize smarter with threat intelligence

To bolster the insights that enable effective prioritization, we now offer a Threat Intelligence Module that allows you to consider which vulnerabilities are being actively exploited. Only 6% to 8% of vulnerabilities actually lead to an exploit that, if not patched, could damage your organization. Our new threat score metric associates this valuable insight with your unpatched products to help ensure you’re aware of those vulnerabilities with the highest risk of exploitation.

To see what applications are covered by the Vendor Patch Module, visit www.flexera.com/svm-vpm.