Ivanti Patch for OEMs

Scan and Remediate Vulnerabilities in Operating Systems and Applications

The Center for Internet Security has listed Continuous Vulnerability Management as the third most important security control behind inventory and control of software and hardware assets. 'Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised.'[1]

The Threat is Real, and Organized

Widespread network attacks made the news in 2017 – WannaCry, Not Petya, and SamSam to name a few. The majority of the impacted companies could have avoided the disruption caused by these attacks if their systems were protected with the latest security updates. For example, the patches for the SMB vulnerability used by WannaCry were available months before the attack and would have prevented the ransomware infection. Caught without a patch and update program in place, WannaCry victims often had to reimage and restore systems from backups if the data was even available.

The Not Petya attack created randon chaos because there was no way to obtain a key for the ransomware, but this was the exception. More attacks are becoming very focused and persistent. According to the 2018 Data Breach Investigations Report, 50% of reported breeches were carried out by organized criminal groups and 76% were conducted for financial gain.[2] To combat this threat, organizations need to include regular scanning to detect vulnerabilities and perform patch deployment as part of their comprehensive security program.

Introducing Ivanti Patch for OEMs

Ivanti provides a patch and remediation software development kit (SDK) you can easily incorporate into your security solution infrastructure.

- Scans for the latest vulnerabilities using Ivanti's award winning patch information content
- Remediates Microsoft operating systems and applications as well as the largest selection of third-party applications in the patch industry
- Minimizes impact on endpoints by conducting quick, efficient scans in seconds and having a small ~ 15 MB footprint
- Supports the latest patch binary download technologies including Microsoft's delta updates
- Provides comprehensive logging to track scanning and installation of patches and to aide in troubleshooting should problems arise
- Optional interaction with end user to show patch activity

[1] Center for Internet Security (CIS), CIS Controls, Version 7, (April 2018)

[2] Verizon Data Breech Investigation Report (April 2018)

Patch and Remediation SDK

The patch and remediation SDK consists of several components, each with an easy to use interface for seamless integration with your security solution infrastructure.

1. **Assessment SDK**
   Performs the scan and detection of product patch status of an endpoint.

2. **Packager SDK**
   Performs the packaging and deployment of updates

3. **Utilities SDK**
   Consists of the Metadata Exporter which queries content about patches and products and Manifest Synchronizer which checks for updated content and SDK components.

These components can be mixed and matched depending upon your security solution infrastructure. While the Assessment SDK is typically incorporated into an agent for the endpoint, the Packager SDK could be used on a central console or integrated with the endpoint agent as well. The Metadata Exporter allows you to display patch information on your management console. The Manifest Synchronizer can also be used to identify when updates are available for any of the SDK components, and facilitate a dynamic download and deployment just like a patch. With this technology, it is easy to keep your security solution up to date.

These components are easily integrated using a Native C structured interface or through a managed interface for higher level languages such as C#.

The interoperability of these components provides the flexibility to match your business needs.

Key Benefits

- Provides patch and remediation to minimize opportunity for exploitation
- Removes the need to monitor and download patches from hundreds of vendors
- Integrates easily into existing security solution framework
- Supports almost any desired workflow to expand and match current product experience

Why Ivanti

Why spend time and resources building features when you can incorporate Ivanti Patch and Remediation into your own solution? As an Ivanti OEM partner, you can enhance your solutions to expand your portfolio and reduce your time to market while delivering increased value for your customers.

Embedding our proven technology enables you to continue to devote resources to developing your core product strengths that add value and set you apart from your competition.

The benefits of working with a leader like Ivanti are clear:

- Proven enterprise-class OEM solutions
- Track record of ongoing OEM relationships
- Flexible business terms
- Regular updates
- Documented roadmap

We make it easier to deliver ahead of the competition.

.