Bitdefender®

Q4
2020

Vulnerability Patching

REPORT BY

ASHISH CHAKRABORTTY, TECHNICAL MARKETING ENGINEER

Table of Contents

Vulnerability Patching

Overview

Patch Management is the practice of reviewing, understanding, testing, deploying, and reconciling the deployment state for software product updates [1]. The goal of Patch Management is to help security professionals identify risks, vulnerabilities, and improve the stability of an IT infrastructure in most environments.

Bitdefender GravityZone integrated patch management module enables organizations to keep operating systems (OS) and third-party applications up to date for workstations and servers. Patch Management module can be added on top of existing Bitdefender GravityZone Endpoint Security products [2]. Integration, simplicity and easy single-console management will enable IT security and operational personnel to focus and work more efficiently.

Technical Diagram

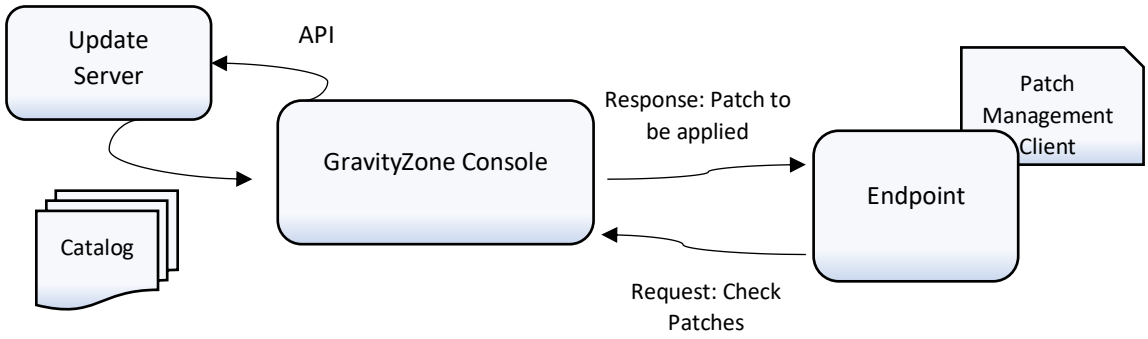

Fig 1: Bitdefender Patch Management workflow

GravityZone Console sources information about the managed patches via the catalog hosted on the update server. It calls an API which returns the hash of the catalog file and the relative path to the catalog file. The console retrieves this file from the specified path, then parses it and inserts the data into collections in patch management database.

Endpoint clients receive patches either automatically or manually after a request is sent to GravityZone console. Security administrators to quickly deploy tested patches from the patch inventory across the entire Windows install base to prevent endpoints from being exploited to a certain OS or application weakness.

Best Practices

A solid patch management process is an essential piece of mature security framework. While patch management is a challenge, it's not impossible. Effective patch management can be summarized as policy, process and persistence [1].

Policy

The first step in developing a patch management strategy is to develop a policy that outlines the who, what, how, when and why of patching clients' systems. The advance planning enables the security teams to be proactive instead of reactive. When a patch management policy is in place, and a notification

arrives of a critical vulnerability in a software product, security professionals will immediately know who will deal with it, how they'll deploy the patch, whether it needs to be done sooner or later, and so on.

Process

The detailed procedure used to respond to vulnerabilities and deploy patches should be explicit within the security policy.

The following six step process is defined as best practice by Microsoft:

Notification: Notification might be sent via email, a pop-up balloon, a message displayed in the web console, or some other method.

Assessment: Based on the patch rating and system configurations, security teams need to decide which systems need the patch, and how quickly they need to be patched to prevent an exploit.

Obtainment: How organizations source the patch they need is dependent on the patch management tool deployed industry wide. These tools range from completely manual to almost entirely automatic.

Testing: Information Testing should always take place before patches are applied to production systems. Patches need to be deployed first on a test bed network that simulates production network.

Deployment: After thoroughly testing the patch, security professionals must carefully deploy them. A good approach is to apply patches one at a time, testing production servers after each patch is applied to make sure applications still function properly.

Validation: The final step involves making sure that the patch has actually been installed on the targeted systems.

Persistence

Policies are useless and process are futile unless IT security persist in applying them consistently. Patch Management is an ongoing closed-loop process and security teams need to constantly apply patches to clients' IT environments. Such a large task is best accomplished following series of repeatable, automated best practices.

Patch Management is a series of best practices that requires:

- Regular discovery of systems that may potentially be affected
- Scanning those systems for vulnerabilities
- Downloading patches and patch definition databases
- Deploying patches to systems that need them

Use Case

Patch Operating System and Applications

Unpatched systems leave organizations susceptible to malware incidents, outbreaks and data breaches. GravityZone Patch Management module enables organizations to keep OS and applications up to date across the entire Windows install base- workstations, physical servers and virtual servers.

Reduce Risks and Attack Surface

Adversaries constantly explore advanced tactics, techniques and practices to exploit OS and application weaknesses to achieve their goals. Bitdefender Patch Management module strengthens the security posture and provisions the security teams to quickly scan affected endpoints and deploy missing security/non-security patches.

Beneficial Outcomes

Flexible and Simplified Patch Management Workflows

Bitdefender Patch Management module supports both automatic and manual patching [2]. It gives organizations greater flexibility and efficiency for patch management, with ability to create a patch inventory, schedule patch scanning, limit automatic patching to admin-preferred applications, vary scheduling for security and non-security patches and postpone reboots for patching requiring a restart

Countless success stories echo Patch Management's superior efficiency, better performance and increased compliance [3]. No supplementary tools are required thereby making Bitdefender the number one choice for a cost-effective solution.

Enhanced Visibility and Reporting

Patch Management provides visibility into systems patching status across entire infrastructure, including the third-party applications, such as Java and Adobe Flash, which don't get picked up by Windows Server Update Services [4].

Administrators can easily run reports and keep the systems updated by applying patches directly from the inventory or the network patch status dashboard. It reduces manual identification and application of patches from weeks to a few hours.

FAQs

Does the security team express concerns about periodically updating patches in your environment?
Bitdefender Patch Management module offers assessment and management of patches for Windows and 3rd party applications. This tool provides visibility into the critical security patch status and enables application of appropriate updates from the inventory in a timely manner.

How wide is the security coverage for your existing Patch Management solution?
Bitdefender Patch Management tool can patch physical and virtual Windows servers, Golden images, Workstations and third-party apps. It is a trusted secure source of patches which includes both security/non-security patches.

Does your patch solution allow specific applications from not receiving updates?
Security practitioners can schedule patch installation and define non-OS third-party applications in the policy to defer them from receiving security/non-security patches. Reboots after patch updates can also be postponed preventing user activity disruption.

References

[1] https://info.connectwise.com/-/media/assets/ebook/patchmanagementbestpractices.ashx
[2] Bitdefender Patch Management Datasheet
[3] Case Study: Archdiocese finds safe-haven from cybercrime with Bitdefender MDR
[4] Case Study: U.K. municipal government elevates security for citizen services