SOLUTION BRIEF

FortiWeb and HPE Security WebInspect

Web Application Vulnerability Scanning and Virtual Patching

Scan. Protect. Patch. HPE Security WebInspect and Fortinet have partnered to deliver a virtual web application patching solution to address vulnerabilities as soon as they're found. Traditionally organizations would need to follow their development process to fix bugs and repair vulnerabilities discovered in their code. This can mean weeks, even months to address serious flaws that could lead to service disruptions and in severe cases, the loss of customer and proprietary data.

FortiWeb's virtual patching uses a combination of sophisticated tools such as URLs, parameters, signatures, HTTP methods and others to create a granular rule that addresses specific vulnerabilities discovered by HPE Security WebInspect. With this multi-faceted approach to rule creation, FortiWeb minimizes the possibility that a scanner-based rule will trigger false positives and prevents impact to overall WAF (Web Application Firewall) performance.

Key Benefits

Using FortiWeb with HPE Security WebInspect gives organizations:

- Less disruptions from emergency fixes and test cycles by virtually patching vulnerabilities.
- Reduced risk of exposure to threats between the time a threat is discovered and when it is fixed by developers.
- Protection for legacy, inherited and third-party applications where development fixes aren't an option or are impractical.
- More stability in application security patches.
- Minimized false detections.

Virtual Patching won't replace the traditional application development process; however, it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application code, such as with legacy, inherited and third-party applications, FortiWeb's virtual patching capabilities can provide a permanent security solution for vulnerabilities.

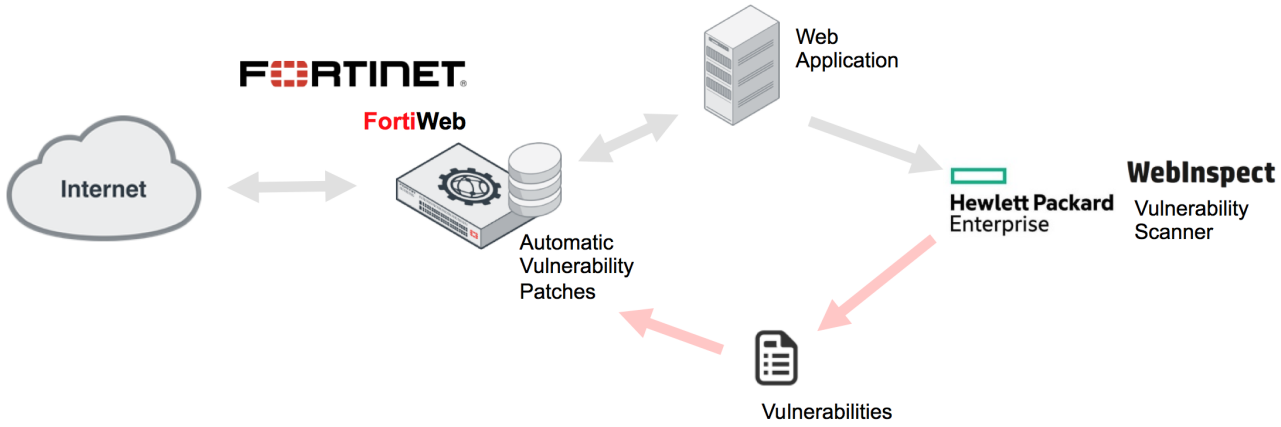

Figure 1: HPE Security WebInspect scan results are imported into FortiWeb; FortiWeb Virtual Patching then automatically creates new rules to protect against newly-discovered vulnerabilities.

Using HPE Security WebInspect to uncover application vulnerabilities provides a comprehensive threat assessment. FortiWeb can now import HPE Security WebInspect results to create custom application protection rules, providing immediate mitigation of identified vulnerabilities. This virtual patching is able to maintain application security until the development teams are able to fully deploy permanent fixes in the application code. It can also extend the time window between security patches to minimize disruptions to the organization and its users.

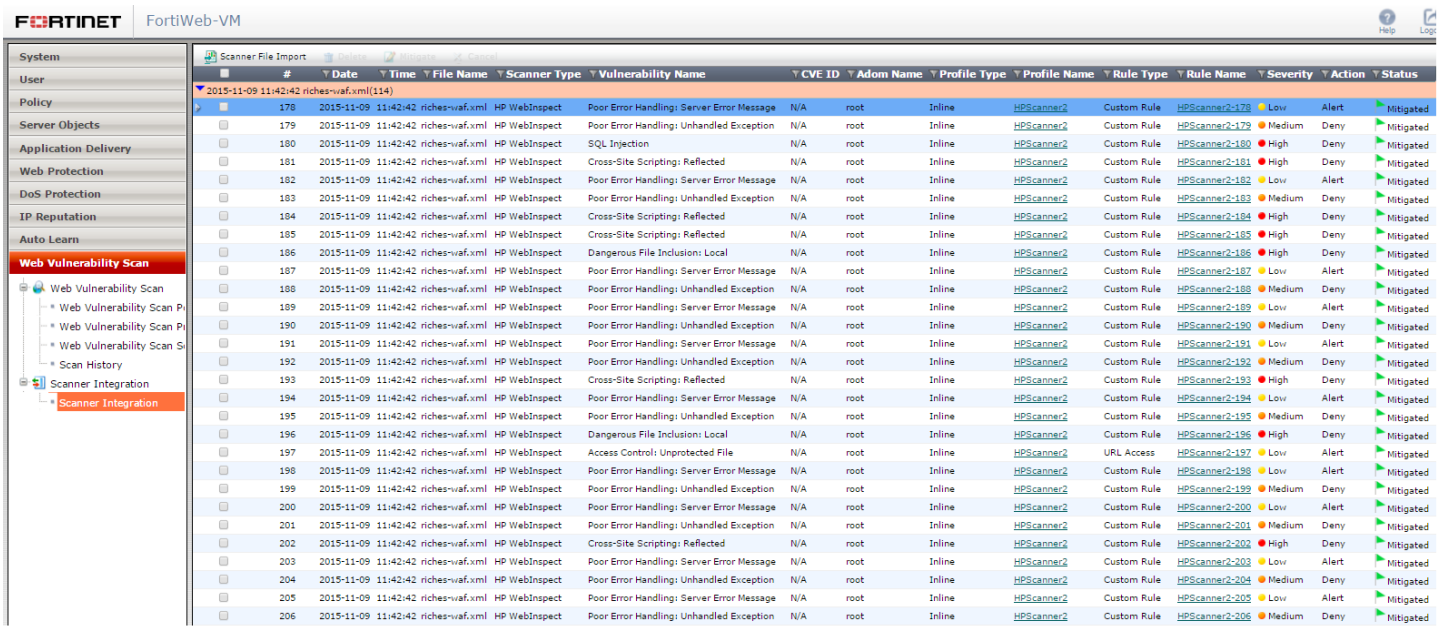

Figure 2: FortiWeb's deep integration with HPE Security WebInspect provides increased user and traffic visibility and provides protection from web application threats.

Use Cases

The integration of HPE Security WebInspect with FortiWeb provides two specific use cases to scan and protect applications from vulnerabilities, as described below.

Temporary Virtual Patching Use Case

In this use case, HPE Security WebInspect scans a web-based application to identify vulnerabilities. The results of this scan are then imported into FortiWeb. FortiWeb analyzes the results of the scan and creates a custom rule for each vulnerability. Each rule is identified by FortiWeb as an HPE Security WebInspect scanner result and is enabled automatically or can be disabled manually by the user. FortiWeb uses these new rules in combination with its other Web Application Firewall services to protect the application until developers are able to release a permanent patch for the vulnerabilities through their normal software development process, eliminating the need for emergency fixes.

Permanent Virtual Patching Use Case

There are many instances where it is not possible or practical to repair vulnerabilities in the application. Third-party, legacy and inherited applications all pose challenges to organizations where they may not have the necessary skills and knowledge internally, or have to engage high-priced outside resources to patch the software. Similar to the first use case, HPE Security WebInspect scans the application for vulnerabilities and the results are imported into FortiWeb. FortiWeb automatically creates rules based on the reported vulnerabilities. These are combined with FortiWeb's Web Application Firewall services to permanently protect the application using FortiWeb's Virtual Patching feature.

Benefits

Using FortiWeb with HPE Security WebInspect gives organizations:

- Less disruptions from emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed.
- Reduced risk of exposure to threats between the time a threat is discovered and when it is fixed by developers.
- Protection for legacy, inherited and third-party applications where development fixes aren't an option or are impractical.
- More stability in application security patches as developers have more time to properly fix code versus issuing emergency patches that haven't had time to be fully tested.
- Minimized false detections based on accurate and verified web application firewall alerts by HP WebInspect.
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by HP WebInspect.
- Additional flexibility and granular management of FortiWeb's Web Application Firewall policies based on scanning results.
- A complete solution for PCI DSS 6.6 compliance.

About Hewlett Packard Enterprise

Hewlett Packard Enterprise is an industry leading technology company that enables customers to go further, faster. With the industry's most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive and more secure. More information about Hewlett Packard Enterprise (NYSE: HPE) is available at www.hpe.com

Fortinet: A Leader in High-Performance Network Security

Fortinet protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments - be it virtualized/cloud or physical. More than 250,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Dec 14, 2016