RBS-2015-003

Bitdefender Multiple Products Missing Revoked X.509 Certificate Validation Spoofing

Table of Contents

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established in early 2011 to better support the many users and initiatives of the Open Security Foundation - including the OSVDB and DataLossDB projects. RBS was created to transform this wealth of security data into actionable information by enhancing the research available, and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database. Available as feature-rich SaaS portal or powerful API

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.

Vulnerable Program Details

Details for the tested product and version:

Vendor:	Bitdefender
Product:	Bitdefender Total Security
Version:	2015 Build 18.21.0.1497

Vendor:	Bitdefender
Product:	Bitdefender Internet Security
Version:	2015 Build 18.20.0.1429

Vendor:	Bitdefender
Product:	Bitdefender Antivirus Plus
Version:	2015 Build 18.20.0.1429

NOTE: Other versions may also be affected.

References

RBS:	RBS-2015-003
OSVDB / VulnDB:	118789[1]
CVE:	N/A

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://www.osvdb.org/show/osvdb/118789

Vulnerability Details

Some Bitdefender products provide HTTPS content scanning used by the parental control and malware scanning features to detect inappropriate or malicious content over encrypted communication. This feature works by installing a root certificate on the system and then acting as a Man-in-the-Middle (MitM) between the user's browser and web servers.

While the feature otherwise properly validates certificates, it fails to check revocation status. This is an important part of certificate validation, as it allows flagging certificates as untrusted if e.g. fraudulently issued or compromised.

Since Bitdefender products do not check this, presenting a previously valid, but now revoked, certificate for a website results in Bitdefender products considering it valid. This allows an attacker able to direct traffic to a malicious site to spoof the identity of another trusted domain for which a revoked certificate is owned. If properly positioned to intercept traffic (MitM), an attacker can also disclose or manipulate traffic between the user's system and a legitimate website.

Solution

According to the vendor, a fix was scheduled for release on the week of Monday, March 2nd.

Timeline

2015/02/20	Approached by IDG News in light of Superfish to check if various security products are affected by similar certificate validation flaws.
2015/02/23	Vulnerability discovered.
2015/02/23	Vulnerability reported to Bitdefender via IDG News contact.
2015/02/23	Vulnerability confirmed by Bitdefender. Fix scheduled for following week.
2015/02/26	Bitdefender accepts publication prior to fixes being available due to current high focus on certificate validation flaws in products and how easy it is to find them. News article published by IDG News.
2015/02/26	OSVDB entry published and details made available on VulnDB[2].
2015/04/29	Publication of this vulnerability report.

[2] https://www.riskbasedsecurity.com/risk-data-analytics/vulnerability-database/