GameHouse RealArcade Installer
Default Game Installation Directory Unsafe Permissions
Privilege Escalation

RBS-2013-005

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

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.

VulnDB - Vulnerability intelligence, alerting, and third party library monitoring and tracking based on the largest and most comprehensive vulnerability database available today. Ability to integrate with products and services via an API or custom export.

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.

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

Security Program Assessment Services / ISO/IEC 27001:2005 - Customized training, security assessments, security program audits, and gap analysis as well as pre-certification consulting services to both protect organizations with best practice security controls and to prepare for a smooth ISO/IEC 27001:2005 certification audit.

Vulnerable Program Details

Vendor:	GameHouse, a division of RealNetworks
Product:	GameHouse RealArcade Installer / ActiveMARK Game Installer
Version:	2.6.0.481 and 3.0.7

References

RBS:	RBS-2013-005
OSVDB:	96918[1]
CVE:	CVE-2013-2604[2]

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://osvdb.org/show/osvdb/96918
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2604

Vulnerability Details

When installing games, the default proposed installation directory is "`%HOMEDRIVE%\GameHouse Games\`". While it may be common knowledge in the IT security industry that installing outside `%ProgramFiles%` may open applications up to trojan-style attacks due to unsafe default permissions, most regular users are not aware of this and are prone to select whichever installation directory is suggested by the installer.

Any application installed within `%ProgramFiles%` inherits permissions that only grant members of the "Users" group permission to "Read & Execute", "List Folder Contents", and "Read". However, installing outside `%ProgramFiles%` - as suggested by the GameHouse installer - causes the installation directory to inherit permissions that grant members of the "Users" group two additional special permissions, specifically:

- Create Files / Write Data
- Create Folders / Append Data

While unprivileged users are not permitted to manipulate or delete existing files, any unprivileged user may create arbitrary files within the installation directory, unless the installer specifically changes the default permissions. The GameHouse installer does not, allowing creation of arbitrary files within the "`GameHouse Games`" folder and subfolders.

The combination of unsafe permissions, allowing unprivileged users to create arbitrary files, and Windows' search order, which specifically looks for libraries loaded with relative paths within the application directory before other directories, may allow any user on the system to execute arbitrary code with the privileges of another user running a game.

This attack has been successfully demonstrated using the game "Zuma Deluxe" as example. By placing a specially crafted library named `DDRAW.DLL` in the "`%HomeDir%\GameHouse Games\Zuma Deluxe`" directory, it was possible for an unprivileged, local user to cause this code to be executed with another user's privileges, when that user attempted to run the game.

Solution

The vendor has not been responsive, so no solution is currently available.

As a workaround, users can during installation select a directory within the %ProgramFiles% path instead of the default suggested game installation path. Limited testing does not show any adverse effects from doing so when playing games.

Timeline

2013/01/26	Vulnerability discovered.
2013/02/13	RealNetworks contacted (clientsecurity@real.com) to obtain GameHouse security contact.
2013/02/15	Security contact requested from GameHouse via their online form.
2013/02/15	Random, off-topic response received from GameHouse customer support: "*I am sorry that you are receiving virus alert when attempted to download games. GameHouse games are tested before release they are safe. If you're receiving a warning message, you may simply need to update your anti-virus software*".
2013/02/15	Clarifying mail sent to GameHouse customer support. No response.
2013/02/21	RealNetworks security contact provides appropriate security contact (DL-games-security@realnetworks.com) for reports related to RealArcade and GameHouse.
2013/03/11	Details sent to GameHouse / RealArcade security contact (DL-games-security@realnetworks.com).
2013/05/29	While not being responsive, GameHouse completes a major site update and provides a new version of the game installer.
2013/07/17	RBS notices the site update and examines the latest version of the game installer. RBS concludes that the vulnerability is still present.
2013/08/13	RBS sends an update to GameHouse to inform about issues still affecting the latest version (DL-games-security@realnetworks.com).
2013/09/05	No response from vendor. VulnDB[3] advisory published as well as "An Analysis of the (In)Security State of the GameHouse Game Installation Mechanism"[4] report.
2013/10/09	Publication of this advisory.

[3] https://vulndb.cyberriskanalytics.com/
[4] http://www.riskbasedsecurity.com/reports/RBS-GameHouseAnalysis-Sept2013.pdf