RiskBased SECURITY

GameHouse RealArcade Installer RACInstaller.StateCtrl.1 ActiveX Control Dispatcher Multiple Methods Use-after-free

RBS-2013-006

gamehouse.

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
Version:	2.6.0.481
Component:	InstallerDlg.dll
Component version:	2.6.0.481

References

RBS:	RBS-2013-006
OSVDB:	96919[1]
CVE:	CVE-2013-2603[2]

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://osvdb.org/show/osvdb/96919

[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2603

Vulnerability Details

The RACInstaller.StateCtrl.1 ActiveX control, {C8F76629-E4F4-4646-AFC0-665082D167B1}, provided by `InstallerDlg.dll` uses its own dispatching functionality called from the `InvokeDispatchWithNoThis()` function in `mshtml.dll`. Instead of dismissing invalid parameter types supplied to methods and properties, the dispatcher attempts to convert these into the correct type by changing the variant type. This behaviour makes it possible to trigger a use-after-free condition that allows arbitrary code execution.

When called, the dispatcher checks the number of arguments supplied before determining which method was called or property specified. If either of the methods listed below are invoked, the function determines if the supplied argument is a string by confirming if the variant type is VT_BSTR.

* `QueueRemove()`
* `QueuePause()`
* `QueueTop()`
* `Ping()`
* `message()`
* `AddTag()`
* `RemoveTag()`
* `TagRemoved()`

Instead of dismissing other input types as invalid and returning an error, as is customary, a function is called to convert the variant type. This is done by eventually calling `VariantChangeType()` after which `VariantClear()` is called to clear the originally supplied variant. In case the variant was an object, this is released, causing its reference count to be erroneously decremented, which may later cause the object to be prematurely freed.

On way of triggering this is by supplying the ‘window’ object to one of the affected methods e.g. `Ping()`. Calling it multiple time, it is possible to decrement the `CComWindowProxy` object’s reference count to zero, causing it to be prematurely freed and then later dereference the memory.

Solution

While the vendor has not been responsive, a new version of the site and game installer was released end of May 2013. Upon review, it was determined that the latest version of the installer, 3.0.7, no longer marks the vulnerable ActiveX control as “safe-for-scripting”.

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, which no longer sets the ActiveX as “safe-for-scripting”.
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