RiskBased
SECURITY

RBS-2019-014

Honey Browser Extension Content Script Improper DOM Handling Browser Action UI Spoofing

Table of Contents

Table of Contents 2

Vendor / Product Information 3

Vulnerable Program Details 3

Credits 3

Impact 3

Vulnerability Details 3

Solution 4

References 4

Timeline 4

About Risk Based Security 5

Company History 5

Solutions 5

Vendor / Product Information

The Honey Browser Extension for Chrome, Firefox, Safari, and Edge allows users to instantly find and apply coupon codes at checkout for over 30,000 online shopping sites and, according to the vendor, 10,000,000 members utilize the extension.

Vulnerable Program Details

Details for tested products and versions:

Vendor: Honey Science Corporation
Product: Honey Browser Extensions for Chrome, Firefox, Safari, and Edge
Versions:

Honey Addon for Firefox version	10.8.1 and 11.1.0
Honey Extension for Chrome	10.8.1, 11.0.2, 11.1.0, 11.1.1, 11.1.2, 11.2.1, and 11.2.2
Honey Extension for Edge	11.1.1.0
Honey Extension for Safari	10.9.0

NOTE: Other versions than the one listed above are likely affected.

Credits

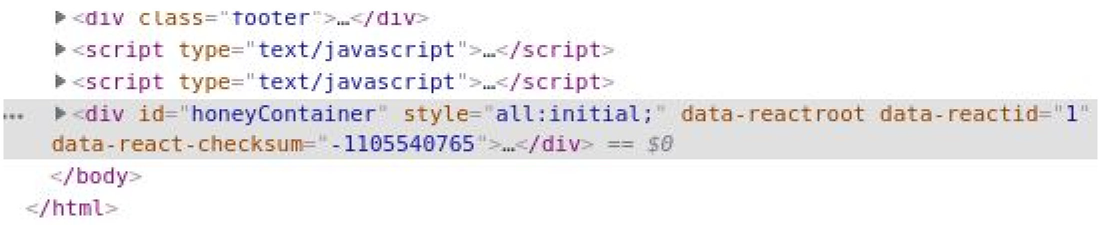
Sven Krewitt, Risk Based Security
Twitter: @RiskBased

Impact

The browser extension’s content script is used to inject and display UI elements in the Document Object Model (DOM) of the current web page. When a user activates the browser action while visiting a specially crafted web site, a context-dependent attacker can spoof UI elements of the browser extension and conduct phishing attacks.

Vulnerability Details

The Honey browser extensions are activated when a user clicks on the Honey extension logo in the browser toolbar. In general, this triggers the browser action defined in the extension manifest and opens a popup window overlay to display extension UI elements. However, the manifest does not specify a window popup, but injects a `div` tag into the current web page's Document Object Model (DOM) tree.



```
    ▶<div class="footer">…</div>
    ▶<script type="text/javascript">…</script>
    ▶<script type="text/javascript">…</script>
…   ▶<div id="honeyContainer" style="all:initial;" data-reactroot data-reactid="1"
    data-react-checksum="-1105540765">…</div> == $0
    </body>
  </html>
```

div tag injected to web page by the Honey extension

As the website controls the DOM tree, it now can also access all injected UI elements from the Honey extension, i.e. the extension's user interface; including the login form. This allows a specially crafted web page to spoof the Honey extension elements and steal user information.

Solution

Update to the following version:

Honey Addon for Firefox version	11.3.5
Honey Extension for Chrome	11.3.0
Honey Extension for Edge	11.4.2.0

References

RBS:	RBS-2019-014[1]
VulnDB:	207147

Timeline

2018-11-21	Vulnerability discovered
2018-12-13	Vulnerability reported to vendor
2018-12-14	Vendor acknowledges the vulnerability
2019-04-16	Vendor releases fix for Google Chrome extension
2019-05-15	Vendor releases fix for Mozilla Firefox extension
2019-06-18	VulnDB 207147 added to VulnDB
2019-07-31	Publication of this vulnerability report

[1] https://www.riskbasedsecurity.com/research/RBS-2019-0XX.pdf

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 to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so 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 in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

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. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

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.