

Webroot endpoint agents under version v9.0.28.48 are vulnerable to the following issues.

CVE-2020-5754 - Type Confusion

This Type Confusion vulnerability is in `wrUrl.dll` which can result in locally or remotely crashing the Webroot service as well as remotely reading contents of memory in the Webroot service. When `wrUrl.dll` is listening for incoming JSON data, an attacker can call "OP" 1, which will result in `wrUrl.dll` traversing the "DATA" list from the attacker's supplied JSON object. The problem is that the elements in the DATA list are not type checked, and instead assumed to be JSON objects themselves. If an attacker passes a LIST object in this "DATA" list, `wrUrl` will attempt to key the "URL" value on a list object. By providing a DATA element of ["URL"], the keying operation of "URL" will succeed, however will mistakenly return the next list element's contents. The next element can be another list which contains a string of an encoded pointer, which will later be dereferenced and its pointer contents will be echoed back to the client in the "URL" output parameter. Below is an example of this via Curl and how it reads the contents of a dll loaded in memory.

Example:

```
curl -X POST --header "Content-Type:application/urldata; charset=utf-8" -d '{"\VER":1, "\OP":1, "\DATA":["[\"URL\"]", [{"\u004c\u0000\u0064\u00731111111111111111"}], "\BRWSR":{"Chrome"}}' 10.0.2.5:27019
```

Response (contents of a dll in memory is returned back over the network):

```
{ "VER":1, "OP":1, "ERR":0, "DATA": [{"URL": "\u25c0!This program cannot be run in DOS mode.\r\r\n$", "CAT.CONF":["0.0"], "BCRI":40, "ALCAT":0, "RTAP":0, "BLK":0, "REF":0}] }
```

CVE-2020-5755 - Local Privilege Escalation

This is due to the %PROGRAMDATA%\WrData\ folder (which contains .dlls that are loaded by the WebRoot service) not being protected against writes. In this scenario, an attacker could trigger the type-confusion bug to crash the service locally, then rename the %PROGRAMDATA%\WrData\PKG to %PROGRAMDATA%\WrData\PKG2, craft their own %PROGRAMDATA%\WrData\PKG directory, and supply their own WrUrl.dll or wrPhreshPhish.dll to hijack the dll when service auto-restarts resulting in privilege escalation to SYSTEM.

Update to Webroot v9.0.28.48

03-16-2020 - Tenable discloses vulnerabilities to Webroot

03-17-2020 - Tenable Follows up, offering extension due to extenuating circumstances

03-17-2020 - Webroot acknowledges disclosure and is investigating issue

04-02-2020 - Tenable follows up asking for update

04-02-2020 - Webroot explains they are in middle of scheduled release, expects fixes to be in released in a next version following the scheduled release

04-03-2020 - Tenable asks for estimated date for the bug fixes release date in order to arrange reasonable extension

04-11-2020 - Tenable follows up, asking for update

04-16-2020 - Webroot responds that they have a build coming next week. Asks if Tenable could confirm fixes

04-21-2020 - Tenable offers to confirm fixes, asks for copy of new build

04-21-2020 - Webroot says they will send build when ready

04-24-2020 - Webroot offers build that has fixed LPE

04-24-2020 - Tenable confirms reported LPE issue has been fixed, but mentions very similar one found that is still affecting the folder structure

04-28-2020 - Webroot responds that it is unlikely to be a problem, since Webroot process is AM-PPL and shutdown of it is unlikely. Webroot asks for 30-day extension so that customers have time to apply the patch

04-28-2020 - Tenable responds that we will not be able to provide an extension once patch is released, due to our disclosure policy. Offers a 2 week extension if they need more development/testing time

04-28-2020 - Webroot responds that they may still need 2 week extension for initial deployment. Asks if Tenable is able to share details of our planned disclosure

04-29-2020 - Tenable offers 2 week extension for an initial deployment, will follow up on details in early June. Points out past disclosures and publications to provide an example of what disclosure details will look like

06-02-2020 - Tenable follows up for update

06-03-2020 - Webroot responds that they are fine for June 15 disclosure, offers input to include in Tenable's disclosure

06-04-2020 - Tenable thanks Webroot for update

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

CVE ID: [CVE-2020-5754](#)

CVE-2020-5755

Tenable Advisory ID: TRA-2020-36

Credit: David Wells



Risk Factor: High

Advisory Timeline

06/15/2020 - Initial Release

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

