6e726d Adding new advisory reports for CVE-2020-25769, CVE-2020-25214. History

1 contributor

1.37 MB

Immunity

Unauthenticated Remote Code Execution in OverwolfUpdater

2020-10-08

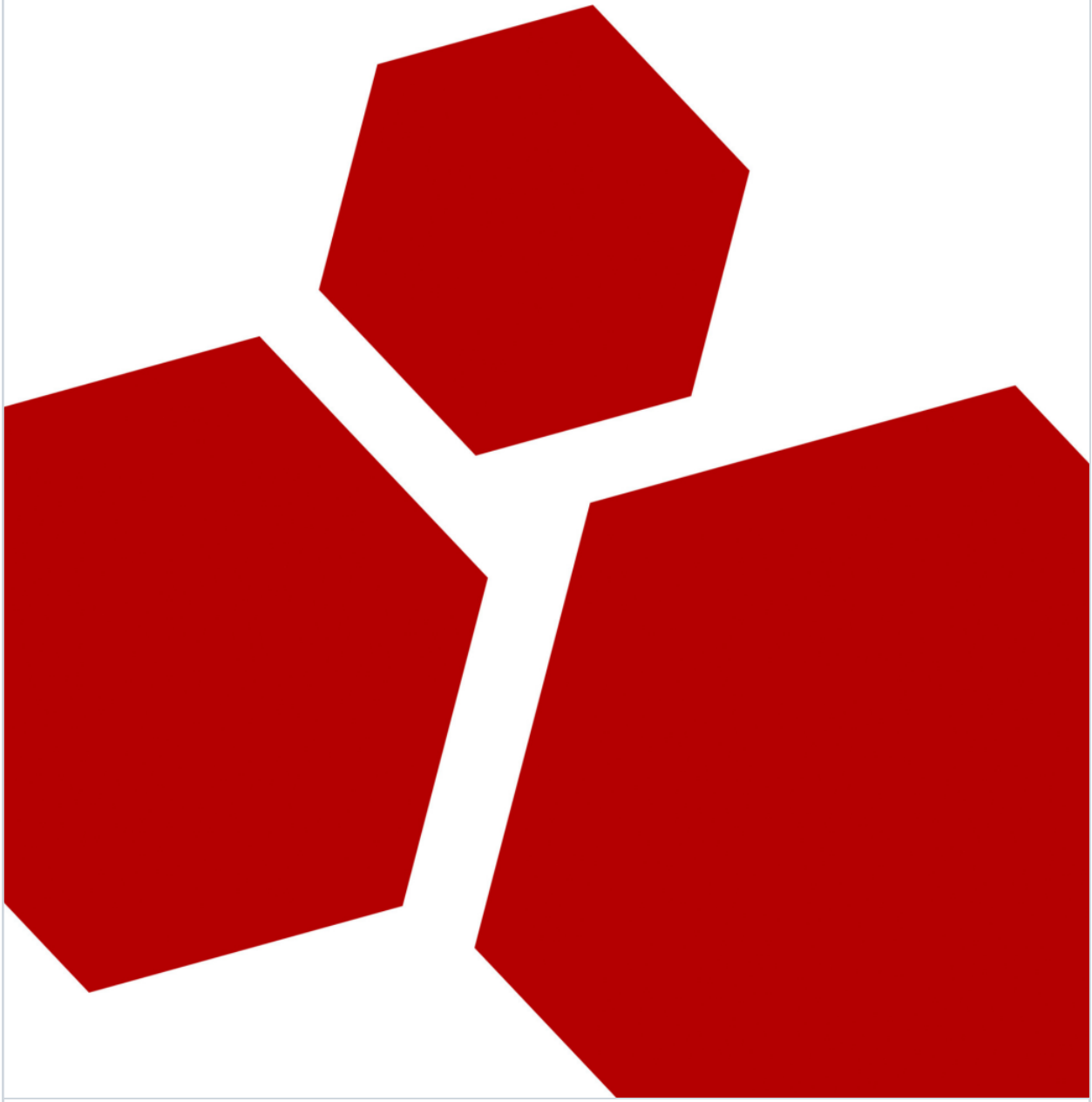


Table of Contents

Advisory Information

Title: Unauthenticated Remote Code Execution in OverwolfUpdater
Vendors contacted: Overwolf Ltd
Release mode: Coordinated Release
Credits: This vulnerability was discovered by Joel Noguera.

Vulnerability Information

Class: Channel Accessible by Non-Endpoint [CWE-300]
Affected Version: Overwolf Client 0.149.2.30 (previous versions may also be affected)
Remotely Exploitable: Yes
Locally Exploitable: Yes
Severity: High - 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE Identifier: CVE-2020-25214

Vulnerability Description

An Unauthenticated Remote Code Execution attack scenario is present within the 'OverwolfUpdater.exe' service. This attack allows malicious users on the same network or positioned in between the user and the remote server to execute code within the target system as the user 'NT AUTHORITY/SYSTEM' and therefore obtaining complete access and control of the machine. In this particular case, attackers will be able to achieve this by performing a Man in The Middle attack against the service while bypassing intended restrictions.

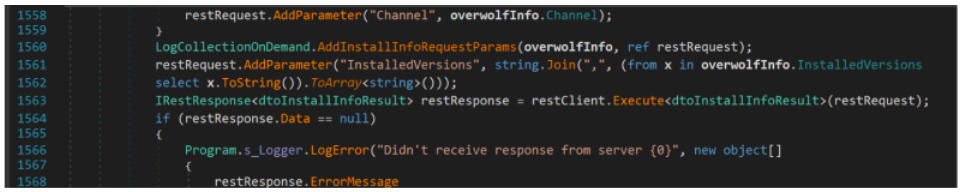
This is achievable because the *'OverwolfUpdater'* service downloads update binaries via an insecure communication channel (HTTP), making possible to swap out the requested binary and the previous HTTP requests with an attacker-controlled binary provided that the attacker is on the same network or positioned in between the user and the remote server. In addition, the file checksum and certificate validation check performed on the downloaded files can be bypassed by remote attackers. Immunity was able to achieve Remote Code Execution on a system in the same network by performing a Person in the Middle (PITM) attack while the vulnerable service was looking for updates.

The update process is triggered constantly and multiple times from the Overwolf.exe process. When this happens, the Service *'OverwolfUpdater'* (OverwolfUpdater.exe) is executed as SYSTEM, and a request to the following URL is made:

URL
http://updates.overwolf.com/install/Info?PartnerID=0&Channel=web_dl_btn2&UID=<UID>&MUID=<MUID>&InstalledVersions=0.149.2.30

Observe that an unencrypted HTTP channel is being used to retrieve the update information. The code in charge of performing this action (Program.GetUpdatesInformation) can be seen below:

```
1550        // Token: 0x060000A6 RID: 166 RVA: 0x00007574 File Offset: 0x00005774
1551        private static dtoInstallInfoResult GetUpdatesInformation(UpdaterOverwolfInfo overwolfInfo)
1552        {
1553            RestClient restClient = new RestClient("http://updates.overwolf.com/");
1554            RestRequest restRequest = new RestRequest("install/Info", 0);
1555            restRequest.AddParameter("PartnerID", PartnersHelper.FetchPartnerIdFromLocalMachineRegistry());
1556            if (!string.IsNullOrEmpty(overwolfInfo.Channel))
1557            {
```



```
1558                restRequest.AddParameter("Channel", overwolfInfo.Channel);
1559            }
1560            LogCollectionOnDemand.AddInstallInfoRequestParams(overwolfInfo, ref restRequest);
1561            restRequest.AddParameter("InstalledVersions", string.Join(",", (from x in overwolfInfo.InstalledVersions
1562            select x.ToString()).ToArray<string>()));
1563            IRestResponse<dtoInstallInfoResult> restResponse = restClient.Execute<dtoInstallInfoResult>(restRequest);
1564            if (restResponse.Data == null)
1565            {
1566                Program.s_Logger.LogError("Didn't receive response from server {0}", new object[]
1567                {
1568                    restResponse.ErrorMessage
```