Starred by 6 users

Owner:	gan...@chromium.org
CC:	sorin@chromium.org adetaylor@chromium.org waff...@chromium.org amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Installer
Modified:	Sep 2, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Merge-na
Needs-Feedback
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-91
Target-91
external_security_report
LTS-Security-90
LTS-Security-NotApplicable-90
Release-0-M92
CVE-2021-30577

Issue 1204811: Security: Local Elevation of Privilege vulnerability in Google Update Service

Reported by reqon...@gmail.com on Sat, May 1, 2021, 2:19 PM EDT

Code

VULNERABILITY DETAILS
A local Elevation of Privilege vulnerability has been discovered in the Google Update Service. This issue can be exploited to obtain SYSTEM privileges on devices that have Google Chrome, or possibly other Google products, installed. The only configuration that is not vulnerable is whenever a user installs Chrome with a low privilege user and does not accept the UAC-prompt in the setup menu. This means that all enterprise configurations in which the Chrome application is installed/pushed to the user from a centralised MDM solution are vulnerable.

VERSION
Chrome Version: 1.3.36.82 (Latest, stable)
Operating System: Windows, all versions. Other operating systems have not been tested.

REPRODUCTION CASE
The vulnerability is quiet straightforward. Whenever Chrome is being installed for all users two scheduled tasks are being created called "GoogleUpdateTaskMachineUA" and "GoogleUpdateTaskMachineCore. These tasks run as SYSTEM as is always the case when "Run whether user is logged on or not" is selected. These tasks are scheduled to run every hour. When the task is run, it checks for the file "GoogleUpdate.ini" on the C:\ root folder.
In this file a user can specify several settings for debugging. One of these settings is the "LogFilePath" value. These settings are specified on your help pages (see: https://support.google.com/chrome/a/answer/6350036?hl=en#zippy=%2Cturn-on-auto-updates-recommended%2Cschedule-auto-updates-outside-of-work-hours%2Ccreate-a-log-file).

When only a filename is being specified the logfile will be written in C:\ProgramData\Google\Update\Log\.
The problem is that a user can enter a full path here and also specify any filename and/or extension that they wish.
When the GoogleUpdate tasks are being executed two things will happen:
1. It checks whether the file exists. If it doesn't, the file will first be created. Then logentries will be appended to the file.
2. The permissions of the file will be altered so that all users have write permissions towards the file.

This procedure is, naturally, being done using SYSTEM privileges. This means a user can abuse this to obtain write-permissions for every file they wish, independent of it's location.
This can exploited in numerours ways. If you want me to make a Proof of Concept in which I showcase that this can be abused to obtain a SYSTEM shell on the machine, I will be happy to do so.

I have attached a PDF with screenshots.

Reproduction steps:
1. On your Windows computer, create a text file called GoogleUpdate.ini.
2. Save the file on the drive root, C:\.
3. Include the content below (where the value of "LogFilePath" can be any file on the system):

```
[LoggingLevel]
LC_UTIL=6
LC_SERVICE=6
LC_CORE=6
LC_NET=6
LC_OPT=6
[LoggingSettings]
EnableLogging=1
```

ShowTime=1
LogToFile=1
AppendToFile=1
LogToStdOut=1
LogToOutputDebug=1
LogFilePath=C:\Program Files (x86)\Google\Update\1.3.36.82\GoogleCrashHandler.exe

4. Wait for the GoogleUpdate task to run (this happens every hour). Or trigger it manually by executing the task for the PoC (requires admin privileges).
5. The specified LogFile is now created and the user has write permissions on it.

I have attached a PDF with screenshots.

Patch suggestion:
The easiest solution would be to change the searchlocation of GoogleUpdate.ini to "C:\Program Files (x86)\Google\Update\".
Another easy solutions would be to completely remove the LogFilePath parameter in the logsettings file.
Last solution would be to prohibit the usage of paths and different file extensions in the value of the LogFilePath parameter.

CREDIT INFORMATION
Reporter credit: Jan van der Put (REQON B.V.)

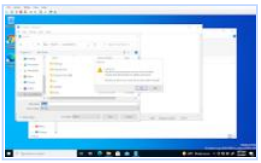
Screenshots - GoogleUpdate EoP.pdf
1.9 MB Download

Comment 1 by sheriffbot on Sat, May 1, 2021, 2:21 PM EDT
Labels: external_security_report

Comment 2 by ajgo@google.com on Mon, May 3, 2021, 12:01 PM EDT
Labels: Needs-Feedback OS-Windows

I think the default permissions on Windows prevent this at Step (2) above - standard users do not have permission to write to c:\ so cannot create this file. Are you sure you are running as a non-Admin (or non-UAC) context?

Capture.PNG
304 KB View Download



Comment 3 by rsleevi@chromium.org on Tue, May 4, 2021, 2:25 PM EDT
Status: Assigned (was: Unconfirmed)
Owner: waff...@chromium.org
Cc: sorin@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable Pri-2
Components: Internals>Installer

waffles: Could you take a look at this? Like ajgo's Comment #2, I'm not fully sure this is an LPE given the current requirements, but I'm tentatively marking this as Medium, in line with the "must already have access to the device" mitigation and consistent with
https://chromium.googlesource.com/chromium/src/+/master/docs/security/faq.md#What-if-a-Chrome-component-breaks-an-OS-security-boundary

Comment 4 by sorin@chromium.org on Tue, May 4, 2021, 2:32 PM EDT
I second the comment #2. Typically, creating the file in the root of C:\ requires elevation.

Comment 5 by sheriffbot on Wed, May 5, 2021, 1:02 PM EDT
Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and medium severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 6 by sheriffbot on Wed, May 5, 2021, 1:38 PM EDT
Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 7 by reqon...@gmail.com on Thu, May 6, 2021, 4:53 AM EDT
Hi, sorry for my delayed reply, I missed the notifcation. I've checked in a fresh Windows install and you seem to be correct that by default a low privileged user has no filecreate permissions on C:\.

However, and I still can't figure out why, ALL the Windows configurations that I have reviewed for clients (20+ different configurations), all provide write permissions on C:\ for standard domain users. No exceptions.
So I thought this might had something to do with it being a domain joined PC, but in my local AD lab this is also not the case.
Now i'm wondering if this has something to do with an enterprise AD management solution like SCCM. I'm currently trying to figure this out by trying to recreate the configuration on our clients.

In any case, even though this might not be exploitable in an out-of-the-box windows installation. If this appears to be exploitable in most (if not all) enterprise AD configurations, then this does pose a serious risk caused by the GoogleUpdate service.

Could you maybe check if the permissions are configured like this in your enterprise AD environment? So not in a separate test-lab. I will also continue researching this myself.

Kind regards,

Jan

Comment 8 by waff...@chromium.org on Thu, May 6, 2021, 9:21 AM EDT
On my enterprise Windows install, I can't write to C:\testfile without elevating.

Still, I agree that there might be some practical benefit to hardening this. Sorin, what do you think?

Comment 9 by reqon...@gmail.com on Thu, May 6, 2021, 12:55 PM EDT
I've just contacted one of our client that does Windows Sysadmin interim jobs for a large number of clients, he confirmed that he has seen write access to C:\ in most configurations he has worked on. He states that this probably has something to do with Windows in combination with SCCM.
I will set up a test lab with SCCM this weekend in order to test this. SCCM is very commonly used and if this causes the change in write permissions this severely impacts the risk of this vulnerability.

Comment 10 by sorin@chromium.org on Thu, May 6, 2021, 12:57 PM EDT

We prefer not making changes to the updater unless there is a proven vulnerability. If we decided to proceed, perhaps the easiest solution would be removing the path altogether. Changing the location of the GoogleUpdate.ini file to "Program Files..." is not practical, since the directory is deleted.

Comment 11 by sheriffbot on Thu, May 20, 2021, 12:21 PM EDT

waffles: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 12 by waff...@chromium.org on Thu, May 20, 2021, 12:25 PM EDT

reqonsec: Were you able to confirm a link with SCCM?

sorin: Should we proceed with removing the path anyways, just in case user write access to C:\ is somewhat common?

rsleevi: What's the proper way to proceed with this bug (in terms of severity, timeline, etc) if it's not a problem with the default configuration of Windows but is a problem for some (an unknown number) of our users?

Comment 13 by reqon...@gmail.com on Thu, May 20, 2021, 12:54 PM EDT

Hi, no not yet. I'm a little short on time. However, I was able to confirm some aspects.
By default, in any Windows configuration, the special identity/group “Authenticated Users” has Write access to C:\. Every user that has authenticated through a sign-in process is part of this identity (https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/special-identities#authenticated-users).
However, the local group “Users” does not have Write access to C:\. I’m not sure what permissions overrule which. But I think the reason all my clients have write access is that they install the Windows OS without any local users and that users will sign-in to the OS using AD. I did not have this set-up ready in my local testlab.
I hope that I have time to confirm this upcoming weekend. Since I understand you want to take actions on this open issue, let’s agree upon the following timeline. I will provide you with an update before next Tuesday. If I can not confirm the reason for the Write access by then, we assume it’s not possible in ‘standard configuration’ and you can rate the issue from that perspective. Is this ok?

Comment 14 by rsleevi@chromium.org on Thu, May 20, 2021, 4:13 PM EDT

Cc: adetaylor@chromium.org amyressler@chromium.org

re comment #12 and severity/timeline: Adrian or Amy should be able to help provide guidance here (was OOO but saw this e-mail fly by, and didn't want to make you wait for a reply)

Comment 15 by adetaylor@google.com on Thu, May 20, 2021, 4:21 PM EDT

waffles@, rsleevi@ invoked me here. I think it's reasonable to assume that this configuration applies to a high enough number of our users that we would consider this a security bug that needs fixing, and even if C: is protected, as I understand it this might allow a user to write to elsewhere on the PC e.g. somebody else's files.

Comment 16 by sorin@chromium.org on Thu, May 20, 2021, 5:16 PM EDT

Owner: gan...@chromium.org
Cc: waff...@chromium.org

Comment 17 by gan...@chromium.org on Tue, May 25, 2021, 5:17 PM EDT

Status: Fixed (was: Assigned)

This is fixed in the GoogleUpdate codebase, and will be shipped with the next release which is expected to be sometime in June.

To mitigate this issue, the fix does the following:
* removes the ability to specify a `LogFilePath` in GoogleUpdate.ini. This implies that the log file will always be GoogleUpdate.log and always under the %ALLUSERSPROFILE%\Google\Update\Log directory.
* checks whether the file is a reparse point after opening the file. The check is made after opening the file, so that the attacker does not get a chance to substitute a reparse point.
* as a defense in depth measure, we check to make sure the parent directory has not been redirected. i.e., the %ALLUSERSPROFILE%\Google\Update directory. We do not check %ALLUSERSPROFILE%\Google and above for reparse points, since an attacker would need to reuse an existing directory structure which has "\Update", which narrows the attack surface considerably, and in addition, we only write to a "GoogleUpdate.log" file within, which is unlikely to affect most applications (such as GoogleUpdate, which has that directory structure under %ProgramFiles (x86)%).

Comment 18 by sheriffbot on Wed, May 26, 2021, 12:47 PM EDT

Labels: reward-topanel

Comment 19 by sheriffbot on Wed, May 26, 2021, 2:07 PM EDT

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 20 by sheriffbot on Wed, May 26, 2021, 2:32 PM EDT

Labels: Merge-Request-92 Merge-Request-91

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M91. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to future beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M92. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 21 by sheriffbot on Wed, May 26, 2021, 2:37 PM EDT

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: Request affecting a post-stable build
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 22 by adetaylor@google.com on Wed, May 26, 2021, 6:21 PM EDT

Labels: -Merge-Request-92 -Merge-Review-91 Merge-NA

Comment 23 by reqon...@gmail.com on Mon, Jun 7, 2021, 10:04 AM EDT

Seems like a great fix for the issue. When will this fix be pushed to stable release? Also, will this report be eligible for a bounty reward? And when will a CVE-number be assigned to this?

Comment 24 by amyressler@google.com on Wed, Jun 16, 2021, 6:50 PM EDT

Labels: -reward-topanel reward-unpaid reward-10000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 25 by amyressler@chromium.org on Wed, Jun 16, 2021, 7:07 PM EDT

Congratulations, Jan! The VRP Panel has decided to award you $10,000 for this report. A member of our finance team will be in touch soon to arrange payment. Very nice finding -- thank you for submitting this issue to us as well as your follow-on analysis and efforts as the team worked on a fix!

Comment 26 by amyressler@google.com on Fri, Jun 18, 2021, 4:50 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 27 by reqon...@gmail.com on Sun, Jun 27, 2021, 3:52 PM EDT

That's amazing! Thanks a lot! I have received the information from the finance team!

Will this finding obtain a CVE number (or some other form of ID)? As a security researcher it is important that I can reference to this finding on my CV.

Comment 28 by adetaylor@chromium.org on Mon, Jun 28, 2021, 12:49 PM EDT

Labels: Release-0-M92

Yes, this will attract a CVE when we mention it in the Chrome release notes.

We'll include it in the release notes for Chrome itself, even though it's actually in the update service and so is released on an independent timeline (as I understand it). I'm labelling this as if we are going to release it in Chrome 92, so that the credit/CVE shows up there.

Thanks for the report :)

Comment 29 by achuith@chromium.org on Mon, Jun 28, 2021, 10:58 PM EDT

Labels: LTS-Security-NotApplicable-90 LTS-Security-90

N/A for LTS since this is Win-only

Comment 30 by reqon...@gmail.com on Wed, Jul 7, 2021, 8:23 AM EDT

Hello, I've a question about the disclosure of this finding. Am I allowed to make a LinkedIn post where I announce that I've discovered a vulnerability in Google Chrome and that $10,000 has been awarded for it? No details about the vulnerability itself, not even the category of the vulnerability.
If this is not allowed. Can I disclosure it without mentioning Chrome? And just stating that i've been given this specific reward from Google?

Comment 31 by reqon...@gmail.com on Wed, Jul 7, 2021, 8:26 AM EDT

*EDIT below (clarified some sentences).

Hello, I've a question about the disclosure of this finding. Am I allowed to make a LinkedIn post where I announce that I've discovered a vulnerability in Google Chrome and that $10,000 has been awarded for it? No details about the vulnerability itself, not even the category of the vulnerability, will be shared.
If this is not allowed. Can I disclose it without mentioning Chrome? I will then only state that i've been given this specific reward from Google.

Comment 32 by adetaylor@chromium.org on Wed, Jul 7, 2021, 8:56 PM EDT

Hi reqonsec@, yes, it's fine to state that:
* you've received a $10,000 bounty
* it's a Chrome security bug

Please don't disclose any more than that, until this is marked 'allpublic' which will be 14 weeks after fixing. Thanks!

Comment 33 by amyressler@google.com on Mon, Jul 19, 2021, 7:17 PM EDT

Labels: CVE-2021-30577 CVE_description-missing

Comment 34 by amyressler@google.com on Tue, Aug 3, 2021, 3:42 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 35 by sheriffbot on Wed, Sep 1, 2021, 1:30 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 36 Deleted

Comment 37 by amyressler@google.com on Thu, Sep 2, 2021, 3:00 PM EDT

~~Issue 1183137~~ has been merged into this issue.

Comment 38 by amyressler@chromium.org on Thu, Sep 2, 2021, 3:04 PM EDT

~~issue 1183137~~ was reported prior to this report and updated to include the CVE ID assigned for this issue; release notes updated to also include attribution and credit the original researcher and bug report