Could not load component 310543 Dismiss

☆ 154856360 other in WearOS

0 people have starred this issue.

Component 310543

ap...@google.com <ap...@google.com> #1 Apr 23, 2020 04:55PM

Created issue (on behalf of sbagchi@purdue.edu).

Summary: Vulnerability in how WearOS handles Intents can cause the wearable to reboot itself. 04:55PM

We have a paper accepted to the Mobisys conference with our technology to exploit the vulnerability and a workaround. The paper is as follows:
Edgardo Barsallo Yi, Heng Zhang, Amiya K. Maji, Kefan Xu, and Saurabh Bagchi, “Vulcan: Lessons in Reliability of Wearables through State-Aware Fuzzing,” Accepted to appear at the 18th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), pp. 1-14, June 15-19, 2020. (Acceptance rate: 34/175 = 19.4%)

Attack scenario:
You have to send Intents at a high rate which causes resource starvation and the Watchdog times out. The Watchdog is a protection mechanism to prevent the wearable from becoming unresponsive; it monitors the system processes in a while(true) loop with a fixed delay between iterations. The Watchdog as well as a set of critical components (like InputManager, ActivityManager, PowerManagerService) run as threads within the System Server process. If the Watchdog finds a component that is hung for more than 60 seconds (the default timeout value), it will call Process.killProcess(Process.myPid()) to send a SIGKILL signal. Because the monitored components share the same process id with the Watchdog as well as the System Server, this essentially means killing the System Server, which causes the device to reboot.

Component:	310426	04:55PM
Status:	New	04:55PM
Reporter:	sbagchi@purdue.edu (sbagchi@purdue.edu)	04:55PM
+CC:	wo...@google.com, sbagchi@purdue.edu (sbagchi@purdue.edu)	04:55PM
Type:	Customer Issue	04:55PM
Priority:	P4	04:55PM
Severity:	S4	04:55PM
Title:	other in WearOS	04:55PM

ap...@google.com <ap...@google.com> #2 Apr 23, 2020 04:55PM

** NOTE: This e-mail has been generated automatically. ** 04:55PM

Thanks for your report.

This email confirms we've received your message. We'll investigate and get back to you once we've got an update. In the meantime, you might want to take a look at the list of frequently asked questions about Google VRP at https://sites.google.com/site/bughunteruniversity/behind-the-scenes/faq.

If you are reporting a security vulnerability and wish to appear in Google Security Hall of Fame, please create a profile at https://bughunter.withgoogle.com/new_profile.

You appear automatically in our Honorable Mentions if we decide to file a security vulnerability based on your report, and you will also show up in our Hall of Fame if we issue a reward.

Note that if you did not report a vulnerability, or a technical security problem in one of our products, we won't be able to act on your report. This channel is not the right one if you wish to resolve a problem with your account, report non-security bugs, or suggest a new feature in our product.

Cheers,
Google Security Bot

Follow us on Twitter! https://twitter.com/googlevrp

+Hotlist:	702027	04:55PM

st...@google.com <st...@google.com> Apr 24, 2020 10:33AM

Component:	310426	310427	10:33AM

Reporter	sbagchi@purdue.edu
Type	Bug
Priority	P2
Severity	S2
Status	Fixed
Assignee	wo...@google.com
Verifier	--
CC	sbagchi@purdue.edu wo...@google.com
Reporter e-mail	--
Requested charity	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

ap...@google.com <ap...@google.com> #3 Apr 24, 2020 10:34AM

Assigned to wo...@google.com.

Could not load component 310543 Dismiss

** NOTE: This e-mail has been generated automatically. ** 10:34AM

Hey,

Just letting you know that your report was triaged and we're currently looking into it.

You should receive a response in a couple of days, but it might take up to a week if we're particularly busy. In the meantime, you might want to take a look at the list of frequently asked questions about Google VRP at https://sites.google.com/site/bughunteruniversity/behind-the-scenes/faq.

Thanks,
Google Security Bot

Status: New Assigned 10:34AM
Assignee: <none> wo...@google.com

mh...@google.com <mh...@google.com> Apr 24, 2020 10:40AM

Priority: P4 P2 10:40AM
Component: 310427 310543 10:40AM

hl...@google.com <hl...@google.com> Apr 24, 2020 11:28AM

+Blocked by: 154921035 11:28AM

ap...@google.com <ap...@google.com> Apr 24, 2020 11:28AM

+Hotlist: 751044 11:28AM

hl...@google.com <hl...@google.com> #4 Apr 24, 2020 11:28AM

Accepted by wo...@google.com.
-Hotlist: 702027 11:28AM

Hi, 11:28AM

Thanks for your report.

I've filed a bug based on your report.

At first glance, this might not be severe enough to qualify for a reward, though the panel will take a look at the next meeting and we'll update you once we've got more information.

In the meanwhile, can you send us the paper, your findings or some sort of PoC?

All you need to do now is wait. If you don't hear back from us in 2-3 weeks or have additional information about the vulnerability, let us know!

Regards,
Hlynur, Google Security Team

Status: Assigned Accepted 11:28AM
Type: Customer Issue Bug
Severity: S4 S2

ap...@google.com <ap...@google.com> #5 May 6, 2020 09:21AM

+Hotlist: 786228 09:21AM

** NOTE: This is an automatically generated email ** 09:21AM

Hello,

Thanks for reporting this bug. We have notified the team about this issue; they will review your report and decide whether they want to make a change or not.

As a part of our Vulnerability Reward Program, we decided that it does not meet the bar for a financial reward, but we would like to acknowledge your contribution to Google security in our Hall of Fame:

https://bughunter.withgoogle.com/rank/hm

If you wish to be added to the Honorable Mentions page, please create a profile here:
https://bughunter.withgoogle.com/new_profile

Your ranking is based on the number of valid reports.

Regards,
Google Security Bot

--

Could not load component 310543 **Dismiss**

How did we do? Please fill out a short anonymous survey (https://goo.gl/IR3KRH).

-Hotlist: 751044 09:27AM

ap...@google.com <ap...@google.com> #6 Jun 24, 2020 05:56PM ⋮

Marked as fixed.

NOTE: This e-mail has been generated automatically. 05:56PM

Hello,

Our systems show that all the bugs we decided to create based on your report **have been fixed**.
Feel free to check and let us know if it looks OK on your end. Thanks for all the help!

Thanks,
Google Security Bot

Status: Accepted Fixed 05:56PM