Intel tackles firmware vulnerability issue

4 May 2017, by Nancy Owano

(Tech Xplore)—Intel has reported details on a firmware vulnerability, but it does not exist on Intel-based consumer PCs.

Dennis Fisher, editor in chief, *On the Wire*, wrote about it on Tuesday.

The bug was in firmware for some of the processors made by Intel for business-class PCs and servers (or what *ZDNet* referred to as "business chips") hit from 2008 on, so if there ever were such an attack it could place corporate customers at risk.

CoreOS security engineer Matthew Garrett was quoted in *Wired*: "The biggest problem is probably going to be in corporate environments, where getting access to a single machine inside the network now lets you get remote desktop access to a large number of client systems."

According to a May 1 report from Intel, there is an "escalation of privilege vulnerability in Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products."

What to do? Requests may need to be made to your machine's manufacturer for a firmware update, but Intel also provided links to guidelines and mitigations.

Intel is talking about a vulnerability sitting in firmware for some of its processors for years yet undiscovered for that time—possibly, according to some reports, said for nine years. Intel said it can allow an unprivileged attacker to gain control of the manageability features provided by these products.

That restive word "firmware" creeps up yet again, and security watchers know it is problematic—difficult to spot right away and difficult to make the problem disappear without OEM cooperation.

In *ZDNet*, CoreOS security engineer Matthew Garrett was quoted as saying "firmware updates are rarely flagged as security critical (they don't generally come via Windows Update), so even when updates are made available, users probably won't know about them or install them."

SemiAccurate in reaction to the patch news stated, "Luckily Intel has some mitigation options for the affected users, that is you, whether you know it or not. They have two fixes for provisioned AMT and non-provisioned boxes, both prevent the issue from happening until the firmware update has been distributed by OEMs."

Intel marked the severity rating in their posting as critical.

What is the nature of the flaw? Intel pointed to three services. The vulnerability lies in the Active Management Technology (AMT), Standard Manageability (ISM), and Small Business Technology (SBT) firmware.

Specifically, Intel stated that "there is an escalation

of privilege vulnerability" on the AMT, ISM and SBT firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6. [Versions before 6 or after 11.6 are not impacted.]

So what can happen under such an attack? Taking advantage of the vulnerability raises privilege issues.

Chris Duckett in *ZDNet* explained further: "The first, found on AMT and ISM units could allow a remote unprivileged attacker to "gain system privileges to provisioned [chips]," Intel said. The second would allow a local attacker to gain "unprivileged network or local system privileges" on chips with AMT, ISM, and SBT."

As Lily Hay Newman in *Wired* put it, "These features are meant to let network administrators remotely manage a large number of devices, like servers and PCs. If attackers can access them improperly they potentially can manipulate the vulnerable computer as well as others on the network."

Intel thanked Maksim Malyutin from Embedi for reporting the issue, and "working with us on coordinated disclosure."

Now for the not-so-bad-news. No exploitation was detected. *Wired* reported: "The search engine Shodan, which indexes internet-connected devices, shows that fewer than 6,500 potentially affected devices are visible on the open internet."

As for advice, Intel provided a number of recommendations with related guidelines on what to look for. There is a guide, and the link is provided, to assess if your system has the impacted firmware. There is also a document link for mitigations. "If a firmware update is not available from your OEM, mitigations are provided in this document: downloadcenter.intel.com/download/26754."

SemiAccurate commented that "Intel has done their part and delivered the updated firmware to OEMs, it is now up to them to do the right thing. Some will." Charlie Demerjian said to "take the official mitigation steps as soon as possible. Then contact your OEMs and strongly suggest that firmware patches for every system, including-out-of warranty systems, would be appreciated by you."

More information: security-center.intel.com/advi… 075&languageid=en-fr

APA citation: Intel tackles firmware vulnerability issue (2017, May 4) retrieved 16 September 2021 from https://techxplore.com/news/2017-05-intel-tackles-firmware-vulnerability-issue.html