Vulnerabilities found in Dell BIOSConnect features within Dell SupportAssist

25 June 2021, by Bob Yirka

Credit: Unsplash/CC0 Public Domain

A team of engineers at computer security company Eclypsium, Inc. has found four vulnerabilities in Dell BIOSConnect features within Dell SupportAssist. They have reported what they found on their website where they have rated the vulnerability as High.

Dell Computer Technology Company is one of the largest makers of personal computers in the world. As part of their efforts to support their customers the company began installing a BIOS-based application called SupportAssist, which, as its name suggests, is meant to allow Dell technicians to assist users remotely. Dell also preinstalls another BIOS app called BIOS Connect on the computers it sells, which allows the company to update the BIOS of the computers its sells. In this new effort, the team at Eclypsium found a security chain vulnerability that could allow what they describe as 'adversaries' to gain access to the boot process of user computers, which could be used to load adversarial software.

Eclypsium reported the problems it found to Dell this past March, and Dell promptly issued a security advisory to its customers and set about working up a fix. Two of the fixes were completed and updated on server-side machines—the other two, once completed, were sent to Dell's cloud site. Those fixes are now available for those customers who have been impacted; those who have Dell auto-updates turned on need not worry as the updates for they have likely taken place already.

The vulnerability involved 129 different Dell devices, from laptops, to desktops and tablet devices and likely impacted approximately 30 million computers around the world. One of the vulnerabilities involved connections between BIOS updates and Dell servers that could allow an adversary to redirect a computer being updated to an adversarial machine. The other three vulnerabilities were listed as overflow vulnerabilities.

Eclypsium's engineers noted on their website that any attack meant to take advantage of the vulnerability would have had to involve redirecting user computers, which made the likelihood of an attack on individual users very remote. Any such attacks would have been far more likely to take aim at large enterprises with a lot of payoff for adversaries.

More information: Dell: www.dell.com/support/kbdoc/nl- … d-https-boot-feature