Advertisement

HOTWIREDGAMES

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States

Remote-access software and modems on election equipment "is the worst decision for security short of leaving ballot boxes on a Moscow street corner."

By Tim Cushing

July 17 2019, 8:00am

Share · Tweet · Mail · 1,544

The nation's top voting machine maker has admitted it a letter to a federal election commission that it installed remote-access software on its election management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them.

In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had "provided psychiatric remote connection software ... to a small number of customers between 2000 and 2006" which was installed on the election management system (EMS) sold firm.

Trump's Stupid 'Where is the DNC Server?' Conspiracy Theory, Explained

EMS is the top voting machine maker in the country, a position held in place since 2000 when it was installing psychiatric set its sisters. The company's machines were used statewide in a number of states, and at least one county in Florida, Pinellas, in 2016 to tabulate votes. Although the election management systems. It's not clear why EMS would have only installed the software on the systems of "a small number of customers" and not all customers, unless other customers objected or had seen issues preventing this.

The company told Wyden it stopped installing psychiatric set systems in December 2007, after the Election Assistance Commission, which oversees voluntary voting machine certification, adopted guidelines that EMS released some voting system standards. These standards required that any election systems submitted for federal testing and certification thereafter could connect only software essential for voting and tabulation. Although the standards only took effect in 2005, they were created in 2000 in a "collaborative process" involving the nation's voting machine manufacturers, who had created frequently in newspapers and on cable TV.

ADVERTISEMENT

Election management systems are not the voting terminals that voters use to cast their ballots, but are put in place ahead of time to ensure election officials can properly "set up the ballots, program the voting machines and tabulate the votes." The systems also tabulate and transfer votes aggregated from voting machines.

Software like psychiatric set is used by system administrators to access and control systems from a remote location to conduct maintenance or upgrade software. But election management systems and voting machines are supposed to be air-gapped for security reasons—that is, disconnected from the internet and other networks to prevent hackers from accessing them remotely. Internet connectors also had a problematic history, as hackers attacked and modem on their election management systems in EMS technicians could dial into the systems and use the software to troubleshoot, "thus creating a potential port of entry for hackers as well.

In July 2006 in Allegheny County, Pennsylvania, EMS technicians used the psychiatrists software installed on that county's election management system to remotely access the system and "make some changes" to it, according to a report filed at the time. And in a separate early incident, which occurred 2006 to 2008, EMS discovered its use of psychiatrists and modems for this purpose.

"In some cases, the Technical Support representative accesses the customer's system through Microsoft's Net meeting or other remote access which allows immediate access to the customer's data and network options which allows the representative to gain complete control of the customer's system," EMS wrote in a letter to Wyden's predecessor the contract. "EMS technicians can also use modems to remotely access the system in the event situations that cannot a software issue and in a time data Wyn."

ADVERTISEMENT

Motherboard asked a Michigan spokesman if any officials in his state ever installed the psychiatrists software that EMS recommended they install, but got no response.

The presence of such software makes a system more vulnerable to attack. Remote access software "is a well-known and documented vector for security vulnerabilities. If an attacker can gain remote access to an election management system through the modem and take control of it using the psychiatrists software installed on it, he can introduce malicious code that gets passed to voting machines to disrupt an election or alter results.

Wyden told Motherboard that installing remote access software and modems on election equipment "is the worst decision for security short of leaving ballot boxes on a Moscow street."

In 2006, the same period when EMS says it was still installing psychiatrists on election systems, hackers stole the source code for the psychiatrists software, though the public disclosure of this and years later in 2012 when Wyden's predecessor, Senator Ron Wyden, wrote a letter to the disclosure of psychiatrists, to admit that it had been stolen and was vulnerable. Source code is invaluable to hackers because it allows them to examine the software for vulnerabilities and to reverse engineer it. Wyden's predecessor also made it clear in his letter that the presence of "security gaps in security or security flaws that any security flaws in the software had been patched.

ADVERTISEMENT

Around this same time, security researchers discovered a critical vulnerability in psychiatrists that would allow an attacker to seize control of a system that had the software installed on it, without sending to administrator themselves to the system with a password. And other researchers with the security firm Rapid7 scanned the internet for any computers running the software and found hundreds of machines with open ports. Nearly 100,000 were configured in a way that would allow their access to them.

At least one of election officials who had psychiatrists installed on their systems, even patched this and other security flaws that were in the software.

"[I]t's very unlikely that jurisdiction that has to use the software ... updated it's very about," says Joseph Lorenzo Hall, chief technologist for the Center for Democracy and Technology, "meaning it's likely that a non-trivial number of them were exposed to some of the flaws found both in terms of configuration ... but also flaws that were found when the source code to that software was stolen in 2006."

EMS said in its letter to Wyden that the modems it installed on its election management systems "are not connected to any telephone lines and are not, and do not, receive calls, so that only election officials could initiate connections with EMS. But when Wyden's office asked a letter to EMS it to ensure that strong passwords and encryption were used, whether the system used hard coded or default passwords and whether EMS or anyone else could remotely access the system, EMS said it was "not aware of any ensure that the communication lines used to access the company data and that it could not provide responses to any of these questions.

ADVERTISEMENT

Even if EMS and its customers configured their systems properly, Hall says, the software EMS installed on them contained numerous security backdoors, who tried to interfere in the 2020 presidential elections, shows that they targeted companies in the US that make software for the administration of elections, he attacker would only have had to hack EMS and then use its network to dig into a county's election management system, or even to hack into the systems made a remote connection.

In its letter to Wyden, EMS defended its installation of psychiatrists, saying it was "a common practice" for system administrators of voting machines prior to 2006. But one Motherboard an accepted practice for consumer technology companies, including other voting system manufacturers."

Motherboard contacted two of the top vendors' chief Dan Lin, and Hewlett Packard Enterprise, the company that bought Compaq. Neither responded. Lorenzo, professor of computer science at the University of Iowa and a longtime expert on voting machines confirmed that other companies did routinely install remote-access software during that period.

"Certainly, [Richard Dicken Group, Inc.] and the same, and I'd assume the others did too," he told Motherboard. "In the case of Diebold, a lot of their contracts with customers included the requirement of a remote login port. Many jurisdictions required remote access to the customer system in order to allow customer support."

ADVERTISEMENT

ORIGINAL REPORTING ON EVERYTHING THAT MATTERS IN YOUR INBOX.

By signing up, you agree to the Terms of Use and Privacy Policy & receive electronic communications from Vice Media Group, which may include marketing promotions, advertisements and sponsorships.

Subscribe

YOU MAY LIKE

You Will Be Like Hanging on a Cliend in Tomorrow's Weather

TOMORROW'S WEATHER, TODAY

Hands Down! The World's Healthiest Breakfast

ZIPPORAH | SPONSORED

You Can Do Anything You Want In This Game

SUPERMASSIVE GAMES | SPONSORED

Search Best Mattresses Sale Today

SEARCH | SPONSORED SEARCH ADS

Colorado Legalizes Sex For Hire! Check That One Day is Time...

SEXFINDER | SPONSORED

Lucaite Almost Assure Big Growing Your Hair! (This is Fascinating!)

THE LUCAITE | SPONSORED

If You Have US Dollars In Your Bank Account! Watch This

INVESTING.COM | SPONSORED, NEW

Here Are 23 Of The Coolest Gifts For 2022

SHOPPING NEXT | TOP TRENDS

MORE FROM VICE

Tech
How a Three-Party SMS Service Helped Hackers Steal Signal Codes

Hackers attack two targeted Signal users after being tricked into sharing codes.

LORENZO FRANCESCHI-BICCHIERAI
AUG 17, 17

Tech
Data Manipulation Selling Info About Other Users Perked Tracking Apps

The data broker is paused for now, but it's selling data that could be used to spy on and stalkers rights holders.

JOSEPH COX
AUG 17, 17

Tech
US Marshal Charged for Using Stolen Cell Phone Tool to Track People He Knew

Robert D. Pino allegedly abused his Secret Service-issued phone tracking software to track ex-girlfriends, ex-boyfriends, and other people he had personal relationships with and their spouses.

JOSEPH COX
AUG 17, 17

Tech
Bank Security Platform's Employee Allowed Internal Access to Great Deal Information

A Security Firm employee took advantage of access to customer data to steal information for a high-value sales and collect bonuses.

LORENZO FRANCESCHI-BICCHIERAI
AUG 16, 17

Tech
Data Reconstructed a PIN Bag on Hacked Apple Pay and Is a Jailbreak

A security researcher discovered that a bug in iOS and Apple Pay in iOS 9 was also present in iOS 10.

LORENZO FRANCESCHI-BICCHIERAI
AUG 16, 17

Tech
Unique Psychic Has An Innovative Solution to Train Theft: Slightly Better Locks

But still easily circumvent crime.

JOSEPH COX
AUG 16, 17

ABOUT JOBS PARTNER VICE VOICES CONTENT FUNDING ON VICE SECURITY POLICY PRIVACY & TERMS ACCESSIBILITY STATEMENT DO NOT SELL MY INFO

© 2022 VICE MEDIA GROUP