# CX All Versions TB CXP-17786: Meltdown and Spectre Exploits Information



## APPLIES TO

| Product | Versions |
|---|---|
| CX-E | All versions |
| CX-S | All versions |
| CX-H | All versions |

## DESCRIPTION

On January 3, 2018, it became public information that many modern CPUs from Intel, AMD and ARM have a couple of serious design issues that could allow malicious code to access the memory of the device and potentially gain access to passwords, encryption keys and other sensitive information. These issues are referred to as Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715).

The three brands of processors are used in servers, workstations, laptops, tablets and mobile phones. So, millions, if not billions, of devices are affected. While the CPUs cannot be fixed, there are mitigating solutions that have been released or are imminent:

- PC vendors are releasing updated BIOS to reduce exposure
- OS vendors are releasing OS updates to reduce exposure
- Browser vendors are releasing browser updates to reduce exposure

All three types of updates should be applied as they become available. None of them fixes the problem, but each mitigates exposure. The most likely avenue of attack is over the web as a website with malicious code can easily exploit the issues just by browsing the website.

Customers should apply any BIOS, OS and browser updates in a timely manner. As with all critical updates, there is no need to wait for us to qualify them first.

### How do the Meltdown & Spectre issues affect our products?

#### CX-E, CX-H, and CX-S

No software updates are necessary. All CX-series products will continue working flawlessly with the OS patches installed.

It is rumored that CPU performance may be adversely affected after applying the OS patches. However, based on statements from Intel and Google, we expect the effect on performance to be nominal and have no effect on capacities. Once the necessary updates are available to us, we will run performance tests to confirm.

**SendSecure**

No software updates are necessary. SendSecure will continue working flawlessly with the OS patches installed.

The potential performance impact of the OS patches will not affect significantly the throughput of the software. It is safe to continue running SendSecure on the same hardware.

The XMedius Cloud team is working at applying the necessary patches to its servers and virtual machines. It is to be noted that SendSecure Cloud runs on AWS and Amazon have already taken the necessary steps to address the issue that could be used to leak information between virtualized instances.

**XMediusFAX**

No software updates are necessary. XMediusFAX will continue working flawlessly with the OS patches installed.

While a vast majority of deployments of XMediusFAX are not going to be impacted by the potential CPU performance downgrade, we are taking further steps to test systems with heavy loads and traffic. As such, if you are running XMediusFAX on hardware that is already stretched to its limit in terms of CPU usage, we recommend that you carefully watch for any change on throughput and on fax delivery failure rate. Once we complete our tests, we will issue a new statement.

The XMedius Cloud team is working at applying the necessary patches to its servers and virtual machines. It is to be noted that part of the XMedius Cloud platform runs on AWS and Amazon have already taken the necessary steps to address the issue that could be used to leak information between virtualized instances.

**Dell Servers (Sold by AVST)**

Dell has created a knowledge base article listing all affected Dell products, including information about BIOS updates for each. Customers with affected Dell servers should download the appropriate BIOS updates from Dell's website (when available) and apply them to their servers.

**Other Hardware (Sold by AVST)**

Telephony and fax boards from Dialogic, Aculab and Brooktrout are not affected.

**Who to contact if you have any questions or concerns?**

**For AVST products**

Please contact your AVST Authorized Reseller for assistance with any questions or concerns you may have regarding the Meltdown and Spectre issues.

**For XMedius products**

Cloud: support.cloud@xmedius.com | https://support.xmedius.com
On-Premises: support.software@xmedius.com | https://support.xmediusfax.com

**FOR MORE INFORMATION**

For any pre-sale questions regarding the CX-Series applications, please contact AVST Sales Engineering at 949.699.2300 or email SalesEngineering@avst.com. For questions regarding installation and implementation, please contact AVST Technical Support:

CX-E and CX-S support: via phone 800.777.2403 or email CXsupport@avst.com
CX-H support: via phone 800.284.3575 or email CXHSupport@avst.com
International support: via phone +44.870.444.8408 or email EuroTS@avst.com