Meltdown and Spectre: Processor (CPU) Speculative Execution Side-Channel Attack Vulnerabilities

This Wiki page contains the latest available information for this vulnerability. Please check back here regularly for updates.

Click **here** to return to the Doc Portal page.

Last update: **11 Jun 2018**

Table of Contents

- Summary
- Ribbon Analysis and Investigation
- Ribbon Products Impacted by Meltdown and Spectre Vulnerability
  - Products Impacted
  - Products Not Impacted
- References

Summary

Ribbon is aware of recently disclosed research regarding side-channel attacks using speculative execution performance optimization in most modern processors (CPUs). These side channel attacks, recently branded as “Meltdown” and “Spectre”, provide a method for an attacker to observe contents of privileged memory, bypassing any expected privilege levels and security checks.

In early January of 2018, it was announced that researchers identified three attack variants (variants 1, 2 and 3) that can exploit vulnerable processors. On May 21st, it was publicly disclosed that researchers discovered two new variants (variants 3a and 4). The current summary of all publicly disclosed Spectre/Meltdown variants are as follows:

- Variant 1: Bounds check bypass (CVE-2017-5753)
- Variant 2: Branch target injection (CVE-2017-5715)
- Variant 3: Rogue data cache load (CVE-2017-5754)
- Variant 3a: Rogue system register read (CVE-2018-3640)
- Variant 4: Speculative store bypass (CVE-2018-3639)

The Spectre attack refers to attack variant one and two, while Meltdown refers to variant three. Many media reports are simply classifying any new variants as Spectre Next Generation or Spectre-NG.

All three CVEs for the first publicly disclosed variants 1, 2 and 3 are rated in the National Vulnerability Database (NVD) as Medium risk with CVSSv2 scores of 4.7 (out of a possible 10). The two new CVEs for variants 3a and 4 are still being assessed in NVD for severity and CVSS score.

In order to exploit any of these vulnerabilities, an attacker must execute crafted code on an affected product. Ribbon products are closed systems which do not allow installation of any unauthorized software. Most Ribbon products and solutions are also deployed in private/trusted and managed networks, with other security access controls and defense-in-depth measures to help mitigate any risks of exploitation.

For customers with Ribbon products running in their own virtualization environment (versus a Ribbon closed/hosted virtualization environment), Ribbon encourages customers to assess the risks and impacts as necessary since these vulnerabilities may also allow a Virtual Machine (VM) instance to glean memory data from the host system (e.g. hypervisor) and other VM instances (tenants/guests).

Ribbon Analysis and Investigation

Ribbon is currently assessing the impacts of these vulnerabilities across its product portfolio and actively following security updates from OS (e.g. RedHat, etc.), processor and virtualization providers as they become available.

Industry analysis regarding these security updates indicate that the updates will most likely introduce **significant** performance penalties (possibly as high as 30%) once applied to products. As such, Ribbon is proceeding prudently with executing in-house capacity benchmark testing in order to quantify the trade-offs between resolution of these vulnerabilities and product performance. Ribbon will communicate these results appropriately via standard product documentation as fixes become available.

Click here to view historical updates...

16 Mar 2018 ***Update:***

Resolutions of Spectre Variant 1 and Meltdown Variant 3 vulnerabilities are now available from most OS vendors (with some OS flavors only having provided resolution for one or the other to date). Given broader industry adoption Ribbon now has increased confidence in the stability of the code updates that are included in these resolutions. As such we are now able to provide patch and/or release update timing for most of our products for Variants 1 and 3. Ribbon continues to perform regression testing and load/capacity benchmarking with these code updates included and in general are forecasting a 2% to 6% decrease/impact to product capacities. Further details on per product impacts will be made available with the patch or updated release information.

Timing for resolution of the Spectre Variant 2 vulnerability is not yet available for most Ribbon products. Intel only recently released its microcode updates to its flow through Hardware/BIOS vendors that are still working to deliver these updates to vendors such as Ribbon. Once updated BIOS/ Firmware is available to Ribbon we will develop regression and load/capacity benchmarking programs along with rollout strategies. Note that resolution of Variant 2 is expected to have greater impacts to product capacities/real-time however the exact range of these impacts is still to be determined. Indications are that some OS vendors are partially mitigating those impacts with software (RetPoline approach).

11 Jun 2018 ***Update:***

Ribbon is currently assessing the resolutions for the new Spectre variants 3a and 4 as they become available from OS vendors and Intel/Hardware platform vendors. Some OS vendors have software based mitigations (patches) available for variant 4, while the mitigation for variant 3a requires a microcode update. A microcode based mitigation will also be supported for variant 4, however, Intel and OS vendors are not recommending it be enabled in most deployments due to the performance impacts versus any additional mitigation benefits.

Resolution plans and timing for the variants 3a and 4 will be updated in this bulletin as they become available.

Ribbon Products Impacted by Meltdown and Spectre Vulnerability

Products Impacted

Table 1: fSonus and fGENBAND Products Impacted by Meltdown and Spectre Vulnerability

No.	Product Name	Former Sonus / GENBAND	Release / Version (Solution Release)	Spectre / Variant 1 (Date & Release)	Spectre / Variant 2 (Date & Release)	Meltdown / Variant 3 (Date & Release)	Comments
1	Application Server (AS)	GENBAND	11.2 (C20 R18)	June 2018		June 2018	
2	Application Server (AS)	GENBAND	12.0 (C20 R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 12.1
3	Application Server (AS)	GENBAND	12.1 (C20 R19)	June 2018 MCP-19.0.20.6 PB		June 2018 MCP-19.0.20.6 PB	

4	C3 Gateway Controller	GENBAND	17	April 2018 ERSD Image		April 2018 ERSD Image	OS Update via Emergency Recovery SD Card image
5	C3 Gateway Controller	GENBAND	18	April 2018 ERSD Image		April 2018 ERSD Image	OS Update via Emergency Recovery SD Card image
6	C3 Gateway Controller	GENBAND	19.1	April 2018 ERSD Image		April 2018 ERSD Image	OS Update via Emergency Recovery SD Card image
7	C15 Compact Softswitch (Call History Server)	GENBAND	All	June 2018 RHEL 6.9		June 2018 RHEL 6.9	Ready to deploy
8	C20 Converged Softswitch (GWC, GVM, SST, CA)	GENBAND	R18	Nov. 2018 R20		Nov. 2018 R20	Upgrade to C20 R20
9	C20 Converged Softswitch (GWC, GVM, SST, CA)	GENBAND	R19	Nov. 2018 R20		Nov. 2018 R20	Upgrade to C20 R20
10	GENView Manager	GENBAND	2 (C20 R18)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
11	GENView Manager	GENBAND	4 (C20 R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
12	GENView - Analytics	GENBAND	1	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Update	
13	GENView - Analytics	GENBAND	2	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Update	
14	G6 Management Module (G6MM)	GENBAND	G6MM for GVM 2.0 BRC (C20 R18)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
15	G6 Management Module (G6MM)	GENBAND	G6MM -13.1 (C20 R18 & R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
16	G6 Management Module (G6MM)	GENBAND	G6MM for GVM 2.0 (C20 R18 & R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
17	G6 Management Module (G6MM)	GENBAND	G6MM for GVM4.0 (C20 R18 & R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
18	General Media Server	GENBAND	1.4.2.x (C20 R18 & R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to R10.x

19	General Media Server	GENBAND	1.7.1.x (C20 R18 & R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to R10.x
20	General Media Server - C20	GENBAND	10.0.10.X (C20 R18 & R19)	April 2018 Patch via VHE Update (Host only)		April 2018 Patch via VHE Update (Host only)	Guest OS updates will be coupled with the C20 R20 / GMS 12.1 Program
21	General Media Server - AS	GENBAND	10.2.X(AS12.1)	July 2018 Patch via PLE4 / Guest OS		July 2018 Patch via PLE4 / Guest OS	
22	MEP	GENBAND	R1.6.1 (C20 R18)	No Resolution Planned	No Resolution Planned	No Resolution Planned	
23	MEP	GENBAND	R1.6.1 (C20 R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	
24	NSP	GENBAND	19 (C20 R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
25	NSP	GENBAND	21 (C20 R19)	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Update	
26	Session Server Trunks (SST) HT	GENBAND	SST17-18 (C20 R18)	No Resolution Planned	No Resolution Planned	No Resolution Planned	
27	Session Server Trunks (SST) MA RMS	GENBAND	R19 (C20 R18)	April 2018 Patch via VHE Update (Host only)	No Resolution Planned	April 2018 Patch via VHE Update (Host only)	Upgrade to C20 R20
28	Session Server Trunks (SST) IA RMS	GENBAND	R19 (C20 R19)	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to C20 R20
29	Signaling Platform 2000 (SP2000)	GENBAND	R3.0	No Resolution Planned	No Resolution Planned	No Resolution Planned	
30	Converged Intelligent Messaging (CIM)	GENBAND	8.2	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9
31	Converged Intelligent Messaging (CIM)	GENBAND	9	May 2018 9.0.2 MR		May 2018 9.0.2 MR	
32	Converged Intelligent Messaging (CIM) VNF	GENBAND	9.1	June 2018 9.1.2 MR		June 2018 9.1.2 MR	
33	G5 SIP Emergency Stand-Alone (ESA)	GENBAND	3	March 2018 3.0 MR		March 2018 3.0 MR	

34	Genview Billing - Mediation	GENBAND	R4.0	No Resolution Planned	No Resolution Planned	No Resolution Planned	Migrate to R6.0
35	Genview Billing - Mediation	GENBAND	R5.0	No Resolution Planned	No Resolution Planned	No Resolution Planned	Migrate to R6.0
36	GENView Assurance	GENBAND	9.x	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 10.x
37	GENView Assurance	GENBAND	10.x	See Comments	See Comments	See Comments	Product is application only in 10.x. Customer provides OS.
38	GENView Manager - OneEMS	GENBAND	1.1	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Update	
39	GENView Manager - OneEMS	GENBAND	2	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Updatee	
40	Provisioning & Portals	GENBAND	9.3	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
41	Provisioning & Portals	GENBAND	9.4	April 2018 Patch via VHE/AVE Update		April 2018 Patch via VHE/AVE Update	
42	Intelligent Messaging Manager (IMM)	GENBAND	4	July 2018 IMM 4.0 PBx		July 2018 IMM 4.0 PBx	
43	SBC (Q10, Q20, Q21)	GENBAND	9.1	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
44	SBC (Q10, Q20, Q21)	GENBAND	9.2	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
45	SBC (Q10, Q20, Q21)	GENBAND	9.3	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
46	SBC (Q10, Q20, Q21)	GENBAND	10	No Resolution Planned	No Resolution Planned	No Resolution Planned	
47	GENView Real-Time Session Manager (RSM)	GENBAND	9.1	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
48	GENView Real-Time Session Manager (RSM)	GENBAND	9.2	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4

49	GENView Real-Time Session Manager (RSM)	GENBAND	9.3	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 9.4
50	QFlex eSBC	GENBAND	6	No Resolution Planned	No Resolution Planned	No Resolution Planned	
51	Qflex EMS	GENBAND	6	No Resolution Planned	No Resolution Planned	No Resolution Planned	
52	SPiDR	GENBAND	4.1	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 4.5 (Q2 2018)
53	SPiDR	GENBAND	4.3	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 4.5 (Q2 2018)
54	Kandy Link / SPiDR	GENBAND	4.4	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 4.5 (Q2 2018)
55	VNF Manager (VNFM)	GENBAND	17.4	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to Cavalli (March 2018 GA)
56	Activation Server (AcS)	Sonus	All	May 2018 11.0.1		May 2018 11.0.1	
57	Access Directory Server (ADS)	Sonus	9.0.8 8.4.18	No Resolution Planned	No Resolution Planned	No Resolution Planned	Product EOL
58	ASX Access Server (Lintel)	Sonus	9.0.8 8.4.18	No Resolution Planned	No Resolution Planned	No Resolution Planned	Product EOL
59	DSC 8000 (SEGway X511)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
60	DSC SWe	Sonus	All	May 2018 R17.0		May 2018 R17.0	
61	DataStream Integrator (DSI)	Sonus	9.3.0	July 2018 9.3.0R0P6		July 2018 9.3.0R0P6	
62	Element Management System (EMS) - IAS	Sonus	10.0.x	No Resolution Planned	No Resolution Planned	No Resolution Planned	
63	Element Management System (EMS)	Sonus	10.1.x	No Resolution Planned	No Resolution Planned	No Resolution Planned	
64	Element Management System (EMS)	Sonus	10.2.x	No Resolution Planned	No Resolution Planned	No Resolution Planned	
65	Element Management System (EMS)	Sonus	10.3.x				Patch back after 11 is complete

66	Element Management System (EMS)	Sonus	11	May 2018 11.0		May 2018 11.0	
67	HA CDR	Sonus	All				
68	Home Subscriber Database (HSDB)	Sonus	All				
69	Interworking Server (IWS)	Sonus	All				
70	Multimedia Communications Server (MMCS)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
71	Multimedia Session Manager (MMSM)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
72	Media Capture Tool (MCT) on Linux	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
73	NetScore	Sonus	All	May 2018 11.0		May 2018 11.0	
74	Promina NX-PSM	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
75	Promina NX-IPTRK	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
76	PSX (Linux)	Sonus	All	May 2018 11.0		May 2018 11.0	
77	SBC Core (51x0/52x0/7000/SWe)	Sonus	All	7.1		7.1	Fix in 7.1 and patch back to 7.0.x & 6.2.x
78	SBC Edge (1000/2000) - with ASM option	Sonus	All	Jan. 2018 January ASM Roll-Up		Jan. 2018 January ASM Roll-Up	
79	SBC SWe Lite	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	Upgrade to 8.0.0
80	SEGway X401e	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
81	SEGway X301	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
82	SEGway X211	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	

83	Service Centralization and Continuity Application Server (SCC-AS)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
84	Session Director (SD)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
85	SGX 4000 (Linux - 4250)	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	
86	SGX 4000 (Linux - HP G8)	Sonus	All	May 2018 10.0.5R0		May 2018 10.0.5R0	
87	Sonus Mobile Client [Downloadable Client (DLC)] – WI-FI Calling	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	Dependent on Client OS & handset
88	Sonus Mobile Client [Downloadable Client (DLC)] – LTE Calling	Sonus	All	No Resolution Planned	No Resolution Planned	No Resolution Planned	Dependent on Client OS & handset
89	VX Series Voice Switches	Sonus	All	Q4 2018 5.2		Q4 2018 5.2	
90	WebRTC	Sonus	1.2.0 1.3.0	No Resolution Planned	No Resolution Planned	No Resolution Planned	Product EOL

Products Not Impacted

Table 2: Products Not Impacted

Product Name	Former Sonus / GENBAND / Third-Party
C15 Compact Softswitch	GENBAND
CS2000 / C20 Converged Softswitch - Call Agent	GENBAND
G5 Line Access Gateway	GENBAND
G6 Universal Gateway	GENBAND
G9 Converged Gateway	GENBAND
Gateway Controller (905)	GENBAND
GSX4000	Sonus
GSX9000	Sonus
Promina NX1000	Sonus
Promina netMS	Sonus
SBC 1000 (without ASM)	Sonus

SBC 2000 (without ASM)	Sonus
SBC Core (51x0/52x0/7000) Baseboard Management Controller (BMC)	Sonus
Sonus Mobile Client [Downloadable Client (DLC)] – WI-FI Calling	Sonus
Sonus Mobile Client [Downloadable Client (DLC)] – LTE Calling	Sonus
T7000 Intellligent Switching System	Sonus
Tenor Series VoIP Gateways	Sonus
HP server platform ILO	Third-Party
IBM STORAGE RAID DS3524	Third-Party
IBM StorWize RAID V3700	Third-Party
Oracle Sun Netra platform ILO	Third-Party
Sun Storage Tek 2540 RAID Storage Array	Third-Party
SecureLink Gatekeeper - VM-based service	Third-Party

Click here to view Table 1 change history...

Table 1 Change History:

- 06 Feb 2018 : Added Admin Portal (AP) and TCS Convergence Server to table 1
- 09 Feb 2018 : Changed "SecureLink Gatekeeper - Standalone physical server" to Impacted, and added recommendation to switch to virtual gatekeeper.
- 12 Feb 2018 : Changed "IBM STORAGE RAID DS3524" and "IBM StorWize RAID V3700" to Not Impacted.
- 14 Feb 2018 : Changed "Promina NX-PSM" and "Promina NX-IPTRK" status to "No update is planned".
- 21 Feb 2018 : Added "5400" to the two SBC Core rows.
- 16 Mar 2018 : Combined fSonus and fGENBAND tables; added additional details.
- 19 Apr 2018 :
  - Added numbered column.
  - Added "GVM, SST, CA" to and removed "ATCA & MA-RMS" from C20 Converged Softswitch (line 8)
  - Added "GVM, SST, CA" to and removed "ATCA" from C20 Converged Softswitch" from C20 Converged Softswitch (line 9)
  - Changed NSP release to 21 (line 25).
  - Added "MA RMS" to SST (line 27). Also changed release to R19; updated "Spectre / Variant 2" and "Meltdown / Variant 3" fields to reflect: "April 2018, Patch via VHE Update (Host only)"
  - Added "IA RMS" to SST (line 28).
  - Changed release date of "Spectre / Variant 1" and "Meltdown / Variant 3" for DSI (line 61) to July 2018.
- 26 Apr 2018 : Adjusted AS Variant 1 and Variant 3 dates and removed release version information to allow for further investigation. (line 1)
- 07 Jun 2018 : Changed Variant 1 and 3 date to June, 2018 with a comment of "Ready to deploy" for C15 Compact Softswitch (Call History Server). (line 7)

Table 2 Change History:

- 16 Mar 2018 : Added table 2.

References

Further information is also available on the following sites:

- https://meltdownattack.com/
- https://www.us-cert.gov/ncas/alerts/TA18-004A
- https://access.redhat.com/security/vulnerabilities/speculativeexecution
- https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

For customers running AWS, please refer to https://aws.amazon.com/security/security-bulletins/AWS-2018-013/.

Click here to view References change history...

Change History

- 12 Mar 2018

  : Added reference link for AWS customers.