NEWS RELEASE

Amulet Hotkey Contacts:

European Editorial:
Tony Hilliard
Tel: +44 20 7960 2400
tony.hilliard@amulethotkey.com

US Editorial:
Stu Robinson
Tel: +1 212.269.9300
stu.robinson@amulethotkey.com

Amulet Hotkey Zero Clients and KVM Extenders Immune to Meltdown and Spectre Vulnerabilities

Zero client and KVM Extender architecture and security benefits simplify IT Incident Management Team response efforts.

London, UK, January 18, 2018 – Amulet Hotkey Ltd., a leader in design, manufacturing and system integration for remote physical and virtual workstation solutions, today announced that DXZ zero client and DX KVM Extender products are not directly affected by recently disclosed Meltdown and Spectre microprocessor vulnerabilities[1].

“We developed the DXZ zero clients and DX KVM Extender host cards from the ground up to meet and exceed the demanding security requirements of government organizations while addressing the graphic and performance needs of users,” said Tony Hilliard, group sales director, Amulet Hotkey Ltd. “confirmation that our client and host card products are immune to the Meltdown and Spectre vulnerabilities demonstrates the benefit these products bring to security conscious organizations.”

“Centralizing workstations and desktops in data centers and replacing them with secure zero clients on user’s desks drives operational and productivity efficiencies,” said David Rule, vice president of technology, Amulet Hotkey Inc. “the benefit for IT Incident Management Teams responding to security events such as this are significant, first avoiding the need to update BIOS and patch OS/software on hundreds or thousands of client devices spread across the entire organization, but also simplifying the process to update centrally located host workstations and servers speeds the time to resolution and reduces costs.“

Meltdown and Spectre are security vulnerabilities that can be used to exploit modern microprocessors to steal data such as secret keys, passwords, valuable IP or sensitive information. These vulnerabilities, called speculative execution side-channel attacks, target microprocessor optimizations that were intended to boost efficiency and performance. The microprocessor architecture flaws can result in malicious code accessing data it should not be able to. Security advisories list affected platforms including Intel, AMD and ARM microprocessors[2,3].

Why DXZ zero clients and DX KVM Extender host cards are not affected:

Amulet Hotkey DXZ zero clients and DX KVM Extender host cards provide remote access to host workstations and systems over standard IP networks by encoding the system display(s), USB and audio. The DXZ zero clients can also be used to access virtual workstation or virtual desktops in public or private clouds. The DXZ zero clients and DX KVM Extenders incorporate Teradici Tera2 PCoIP processors for the host encoding and the associated client decoding at the user's desk.

Meltdown and Spectre attacks require malicious code to be running locally on target microprocessors that support *out-of-order execution* and *speculative execution from branch prediction*. However, zero client and host card architecture does not permit the installation and execution of user applications. Also, Teradici have confirmed that the MIPS processors models used in Tera2 PCoIP processors are not impacted by the exploitation techniques described in the Meltdown and Spectre vulnerabilities[1].

By design, zero clients and host cards are simple and stateless endpoints to enhance security while simplify management and reduce costs. The PCoIP remote display protocol is implemented in hardware using purpose built processors with the following benefits:

- No Windows or Linux OS, GPU drivers or APIs such as DirectX or OpenGL to patch/update.
- No x86 processor/GPU, no local applications or web browser to eliminate common exploits.
- No hard disk drive or local storage to eliminate risks associated with data residing in remote PCs, laptops, thin clients, or tablets.

Important note: *While zero clients and KVM extenders are not directly affected by these vulnerabilities, they can be used to provide a remote access connection to host systems such as workstations, virtual workstations, virtual desktops or cloud desktops that may be vulnerable. These host systems must be protected accordingly.*

Impact to Amulet Hotkey Server and Workstation Products

Amulet Hotkey CoreStation® workstation and server products incorporate Intel microprocessors and GPUs that are impacted by these vulnerabilities[4]. Customers are encouraged to review the following product notice to understand the risks and take the appropriate action to protect themselves and their organizations. See: Meltdown / Spectre vulnerabilities and impact on Amulet Hotkey products

Amulet Hotkey DXZ zero client and DX KVM Extender host key benefits:

DXZ zero client models: DXZ4, DXZC, DXZC-C, DXZC-A series, DXZC-E series, DXR-Z4
DX KVM Extender host and remote workstation cards: DXM series, DXH4, DXP4, DXR-H4, DXT-H4

Key Benefit	Applies to:	
	DXZ	DX
Extensive Endpoint Security - Only display pixels are sent to the client allowing application data to remain locked down in a secure data centre. Many security features including: unique USB security authorization, strong encryption and more.	•	•
NCSC CPA and NATO Certification –DXZC-A zero client series are certified as secure for Remote Desktop Security Characteristic version 1.0 at Foundation Grade. See NCSC Certificate #: RDT5722298 and NATO Information Assurance Product Catalogue listing.	•	
Mission Critical Design – The DXZ clients and DX host cards are TAA compliant and engineered for security, reliability, and strict emissions control. Model options for RJ45 copper network connections, or SFP slots for either copper or fibre modules.	•	•
Host system isolation –DX host cards encode displays using the digital video output from the host system GPU to avoid interaction with the host CPU or applications. The DX card network interface is dedicated for PCoIP traffic only for host isolation and for security by separating host system and PCoIP network traffic.		•
Non-intrusive KVM Extension – the DXR-H4/DXT-H4 KVM Extender host cards connect to		•

host systems using standard external cables for security or when it is not possible to install a remote access PCIe card or software.		
Flexible deployment – The DXZ clients support a variety of users across multiple locations connecting to remote physical or virtual 3D workstations, VMware Horizon virtual desktops and applications, or Amazon Web Services Workspaces cloud desktops. The DX host cards provide remote access for any system with digital video outputs.	•	•
Exceptional user experience – The DXZ clients support a range of users from mainstream office desktops to the highest performance 3D graphics. DX host card uses hardware remote display protocol encoding to ensure a responsive experience for the most demanding users.	•	•

For more information visit http://www.amulethotkey.com, or contact Amulet Hotkey.

About Amulet Hotkey

Amulet Hotkey is a proven innovator in design, manufacturing and system integration of high availability solutions for remote physical or virtual workstation, as well as virtual and cloud desktop that are optimized for both mission and business critical applications to deliver robust, secure and uncompromised performance backed up by world-class support. Amulet Hotkey partners with leading manufacturers of data center, cloud and virtualization technologies that enable them to bring to market unique solutions tailored to enterprise IT needs for a truly flexible and scalable computing architecture. Amulet Hotkey customers include Fortune 500 and Global 2000 enterprises as well as local and federal governments. The Amulet Hotkey solutions are deployed in command and control, emergency call centers, investment banks, oil & gas, CAD designers, digital content creation, and post production studios around the world.

Amulet Hotkey was founded in 1990, and is headquartered in the UK where design and manufacturing facilities are based with sales, support and technology centers in London and New York. For more information see www.amulethotkey.com.

1. https://techsupport.teradici.com/ics/support/kbAnswer.asp?questionID=3250
2. Google Project Zero blog post
3. CERT/CC Vulnerability Note VU#584653
4. https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr