VASCO Security Advisory

Meltdown and Spectre Vulnerabilities in IDENTIKEY Appliance and IDENTIKEY Virtual Appliance

Advisory ID: vasco-sa-20180118-meltdown-spectre-ia-iva

Revision number: 0.4

Date and time of release: January 18 2018 17:00 UTC

Date and time of last update: January 19 2018 12:00 UTC

Summary

The Meltdown and Spectre vulnerabilities, which affect Intel, AMD and ARM processors, allow unprivileged rogue processes to read kernel and user programs memory, which may allow malware to steal passwords, cryptographic keys or other confidential information.

Because they are using or are highly likely to rely on vulnerable processors, both the IDENTIKEY Appliance and IDENTIKEY Virtual Appliance products are exposed to these vulnerabilities. However, the risk of exploitation is low.

Impacted products

The following VASCO products are affected by the Meltdown and Spectre vulnerabilities:

- IDENTIKEY Appliance 3000 Series, 5000 Series, 7000 Series
- IDENTIKEY Virtual Appliance 1000 Series, 2000 Series, 4000 Series, 8000 Series

Detailed description of vulnerability

Exploitation of the Meltdown and Spectre vulnerabilities can only be done by dedicated malware running either on the appliance or on the computer hosting the virtual appliance. Such malware must have been installed and run exploiting other security flaws. A typical attack scenario involves the attacker to be authenticated and to have the right to execute code.

IDENTIKEY Appliance does not allow shell access, not even for administrators. Therefore, it is unlikely that malware is installed and run and the probability of exploitation is low. Regarding IDENTIKEY Virtual Appliance, the probability of exploitation further depends on the security of the host computer and the hypervisor. However, the appliance typically stands on a local network behind a firewall and benefits from security controls put in place locally such as e.g. authentication and access control.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of the Meltdown and Spectre vulnerabilities in the context of IDENTIKEY Appliance and IDENTIKEY Virtual Appliance.

CVSS Base Score: 1.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Local	High	Single	Partial	None	None
CVSS Temporal Score: 0.8					
Exploitability		**Remediation Level**		**Report Confidence**	
Functional		Official fix		Confirmed	

Product fixes and workarounds

Customers using IDENTIKEY Appliance should apply the IA update package version 3.14.15, which will patch the operating system of the appliance.

Customers using IDENTIKEY Virtual Appliance should apply the update package version 3.14.15, apply patches for the operating system of the host and also patches for the hypervisor (VMWare, Citrix or Microsoft virtual environment).

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from MyMaintenance.

References

Official website about the Meltdown and Spectre vulnerabilities: https://meltdownattack.com

Legal disclaimer

WHILE EVERY REASONABLE EFFORT IS MADE TO PROCESS AND PROVIDE INFORMATION THAT IS ACCURATE, ALL THE CONTENT AND INFORMATION IN THIS DOCUMENT ARE PROVIDED "AS IS" AND “AS AVAILABLE,” WITHOUT ANY REPRESENTATION OR ENDORSEMENT AND WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OF CURRENCY, COMPLETENESS OR SUITABILITY, OR ANY WARRANTY INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE. YOUR USE OF THIS DOCUMENT, ANY INFORMATION PROVIDED, OR OF MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. VASCO RESERVES THE RIGHT TO CHANGE OR UPDATE THE INFORMATION IN THIS DOCUMENT AT ANY TIME AND AT ITS DISCRETION, AS AND WHEN NEW OR ADDITIONAL INFORMATION BECOMES AVAILABLE.