



CVE-2018-17765

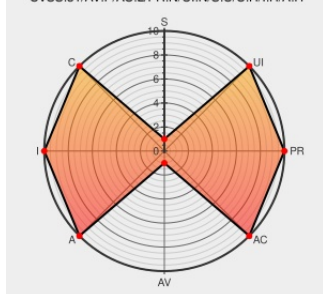
Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 08:54:00 PM UTC

CVE-2018-17765

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of **Telium 2** from **Ingenico** contain the following vulnerability:

Ingenico Telium 2 POS terminals have undeclared TRACE protocol commands. This is fixed in Telium 2 SDK v9.32.03 patch N.

CVE-2018-17765 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Ingenico Group - Smart Terminals - Telium2	Product ingenico.us text/html	MISC ingenico.us/smart-terminals/telium2
DEF CON Safe Mode Payment Village - Aleksei Stennikov - PoS	Exploit	MISCyoutu.be/gtbS3Gr264w

Third Party Advisory
youtu.be
text/html

Exploit
Third Party Advisory
youtu.be
text/html

[www.ptsecurity.com](http://www.ptsecurity.com/text/html) MISC www.ptsecurity.com/en/analytics/threatscape/pt-2020-14/

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ingenico	Telium 2	-	All	All	All
Hardware	Ingenico	Telium 2	-	All	All	All
Operating System	Ingenico	Telium 2 Firmware	All	All	All	All
Operating System	Ingenico	Telium 2 Firmware	All	All	All	All
cpe:2.3:h:ingenico:telium_2:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:ingenico:telium_2:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:ingenico:telium_2_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:ingenico:telium_2_firmware:~::~~::~~::~~::~~::~~::~~:::						

[← Previous ID](#)

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report