

Acer under fire: Now hackers claim to have hit Acer Taiwan, too - DataBreaches.Net

Published: 2021-10-16 · Archived: 2026-04-09 02:14:38 UTC

DESORDEN threat actors are still going after Acer, it seems. In addition to their [recent revelation that they exfiltrated 60 GB of data from Acer India](#) — a breach that Acer confirmed — they have alerted DataBreaches.net that they have also successfully attacked Acer in Taiwan. In a statement to DataBreaches.net, the threat actors write:

To prove our point that Acer is way behind in its cyber security effects on protecting its data and is a global network of vulnerable servers. We have hacked and breached Acer Taiwan server, storing data on its employee and product information.

As proof of claim, they provided links to some data, including a file that does appear to be Acer Taiwan employee data.

DESORDEN claims that they did not steal all data, and “only took data pertaining to their employee details.”

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	userid	createuserid	modifyuse tel		name	email	enabled	password	cellphone	createdat	depart_sn	modifydat	depart_na	is_exec_di	is_exec_nc
2							1				16			1	0
3							1				80			1	0
4							1				6			1	1
5							1				68			0	0
6							1				5			1	0
7							1				13			1	0
8							1				39			1	0
9							1				3			1	0
0							1				45			0	0
1							1				0			1	1
2							1				3			1	0
3							1				13			1	0
4							1				3			1	1
5							1				2			1	0
6							1				8			0	0
7							1				9			1	1
8							1				38			1	0
9							1				8			0	0
10							1				38			1	0
11							1				5			1	0
12							1				1087			1	0

Image: Some of the alleged employee data from Acer Taiwan, redacted by DataBreaches.net.

“Right after the breach, we informed Acer management on the Taiwan server breach and Acer has since taken the affected server offline,” they added.

DataBreaches.net has reached out to Acer Taiwan for comment, but did not receive an immediate reply. This site has also asked DESORDEN to clarify what their actual goal is with respect to Acer and how much ransom they have been demanding. DESORDEN replied that they did not make a demand for separate payment for the Taiwan breach. “We informed them to close the vulnerability,” they explained.

DESORDEN’s message ended with a somewhat ominous note for Acer:

Also, a few other of its global networks including Malaysia and Indonesia servers are vulnerable too.

This post will be updated when a reply is received from Acer Taiwan. In the meantime, DESORDEN also posted their claims to a popular forum for trading, sharing, and selling data.

Updated at 2:13 to include DESORDEN's explanation that there was no separate payment demand associated with the Taiwan attack.

Updated October 18: DataBreaches.net has received the following statement from Acer:

We have recently detected an isolated attack on our local after-sales service system in India and a further attack in Taiwan. Upon detection, we immediately initiated our security protocols and conducted a full scan of our systems. We are notifying all potentially affected customers in India, while the attacked Taiwan system does not involve customer data. The incident has been reported to local law enforcement and relevant authorities, and has no material impact to our operations and business continuity.

Best regards,

Steven

Acer Corporate Communications

DataBreaches.net has sent a follow-up inquiry asking whether Acer will be notifying employees, and what it is doing proactively in light of DESORDEN's claims that other Acer units are vulnerable, too. Acer's spokesperson replied:

As this is an ongoing investigation and for the sake of security, we are unable to comment on details, but potentially affected parties are being notified. Upon detection, we immediately initiated our security protocols and conducted a full scan of our systems. The incident has been reported to local law enforcement and relevant authorities.

Source: <https://www.databreaches.net/acer-under-fire-now-hackers-claim-to-have-hit-acer-taiwan-too/>