

Security Vulnerability Report Form					
Must	Required for initial assessment; enter Unknown if uncertain.				
Optional	Provide if available; may be supplemented later.				
No.	Requirement	Information requested	Instructions	Customer response	Attachment reference
A. Reporter & timing					
1	Must	Reporter company	Legal company name and country		
2	Must	Contact person	Name, title, email and immediately reachable phone number		
3	Optional	Relationship	End customer / Distributor / System integrator / Other		
B. Product identification					
4	Must	Product model	Enter the complete model number		
5	Must	Serial number(s)	Enter serial number(s) or a range if available; otherwise enter Unknown		
6	Must	Product Information	BIOS, OS, firmware, installed software, customized components		
7	Optional	Affected quantity	Number of units; enter an estimate if uncertain		
8	Optional	Product location	Country, city and customer site; country is the minimum required		
C. Incident and impact					
9	Must	When was the issue first detected?	YYYY-MM-DD HH:MM + time zone		
10	Must	Is the incident ongoing?	Yes / No / Unknown		
11	Must	Incident summary	Describe what happened, how it was detected, and the current status		
12	Must	Were important data, functions or product security controls affected?	Yes - Confirmed / Yes - Suspected / No / Unknown. Consider availability, authenticity, integrity, confidentiality, authentication, access control, encryption, BIOS, BMC, firmware and OS		
13	Must	Was malicious code introduced or executed?	Yes - Confirmed / Yes - Suspected / No / Unknown. Consider the product and the user's IT/OT network		
14	Must	Reproduction steps or scripts	Provide detail instruction for us to reproduce it, enter Unknown if uncertain		

Security Vulnerability Report Form					
Must	Required for initial assessment; enter Unknown if uncertain.				
Optional	Provide if available; may be supplemented later.				
No.	Requirement	Information requested	Instructions	Customer response	Attachment reference
15	Must	Known vulnerability information	If exploitation of a known vulnerability is suspected or confirmed, provide available CVE ID, CWE ID, CVSS version/score/vector, references and supporting evidence, enter Unknown if uncertain		
16	Optional	Data affected	Data type, sensitivity and whether personal data may be involved		
D. Evidence & response					
17	Must	Evidence currently available	Logs / EDR alert / IOC / Screenshot / Packet capture / Forensic image / None / Unknown		
18	Optional	Immediate actions taken	Isolation, shutdown, blocking, password reset, update or other action; enter None if no action was taken		
19	Optional	Indicators of compromise (IOC)	IP addresses, domains, URLs, file hashes or other indicators		
20	Optional	Authorities already notified	CSIRT, data protection authority, police or other authority, including notification time		
21	Optional	Additional notes	Open questions, contact restrictions or other relevant information		
Submission reminder: Fill in all "Must" columns. Submit all currently available information immediately. Clearly enter Unknown where the root cause or another required item is not yet known. This form does not constitute an admission of product defect, non-conformity or legal liability.					