THREAT ONTOLOGY

Threat ID	202336371
Threat_Code	GDK001-2245-0099
Threat_Category	External-To-Internal (ETI)
Threat_Class	**High Impact (Risk Value=22)**
Threat_Type_ID	MDB-0774 (Max Penetration)
Threat_Short_Name	MonetDB Exploit
Threat_Long_Name	External Attacker exploits internal database using crafted SQL statements.
Threat_ Description	GDKfree component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause denial of service (DOS) via crafted SQL statements.
Main Actor(s)	External Attacker.
Countermeasure Control Unit(s)	FRS-2932 First Response Salvo; AIE-1187 AI Engine Response; SMA-3400 Senior Management Alert; KB-3601 Knowledge Base Update;
Threat_Impact_Id	TI-7691
Threat_Response_Id	TR-0899
Threat_Contingency_Id	TC-7665; TC-0321; TC-2222
Threat_Precondition(s)	Fragility existed and exploited
Threat_ Postcondition(s)	Damage to enterprise networks/servers/applications materialized
Threat_Related_Id(s)	000100122377; 000100122380; 000100122379; 000100122111; 000100122869; 000100126522 000100126900; 000100122872

Risk Management Engine	Occurrence	Impact	Response
	1.0 Unbunto Server Admin Console displays error message (500 Internal server error)	**1.1** Corporate Website is down **1.2** SAP Portal is down **1.3** East Wing WIFI Cameras beeping – No Signal **1.4** HELPDESK Portal is down	**1.1.1** Invoke FRS-2932 First Response Salvo **1.1.2** Invoke AIE-1187 AI Engine Response **1.1.3** Invoke SMA-3400 Senior Management Alert **1.1.4** Update KB-3601 Knowledge Base

RISK Assessment Analysis and Reporting			
	2.0 Assess Impact	5.0 Assess Response	8.0 Update Disaster Recovery Plan
	3.0 Analyze Impact	6.0 Analyze Response	9.0 Update Countermeasure Plan
	4.0 Report Impact	7.0 Report Response	10.0 Update Risk Management Plan