国际电信联盟

ITU-T

国际电信联盟 电信标准化部门 X.1367 (09/2020)

X系列:数据网、开放系统通信和安全性 安全应用和服务(2)-物联网(IoT)安全

物联网(IoT)安全事件操作的错误日志标准格式

ITU-T X.1367 建议书



ITU-T X 系列建议书

数据网、开放系统通信和安全性

	发机1177700011117 人工压	
田本美色生産	↑ 田 粉 田 図	V 1 V 100
M미元語 X.300 X.399 경息处果系统		
お見か理系統		
日前線		
SON법에 제系統概範	W = 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	
SSI管理		
安全		
SSI应用		
田政分布式处理		
信息和网络安全		
一般安全问題		A.900–A.999
网络安全 安全管理		V 1000 V 1020
文全管理 生物測定 安全施川和服务 (1) 組構安全 家庭网络安全 大数属安全 知1120-X1119 移动安全 X1110-X1119 对等网径安全 X1110-X1119 网络身份安全 网络身份安全 X1110-X1119 网络空间安全 网络安全 反战数信息 身份管理 安全应用和服务 (2) 应急通信 没在使滤器网络安全 X1200-X1229 安全应用和服务 (2) 应急通信 设在传滤器网络安全 X1300-X1249 身份管理 安全应用和服务 (2) 应急通信 资格管理 安全应用和服务 (2) 应急通信 多价管理 安全应用和服务 (2) 应急通信 次在或器网络安全 X1300-X1399 设证邮件 X1310-X1319 为诉武帐神技术安全 为布式帐神技术安全 X1300-X1399 对作式帐神技术安全 X1300-X1399 对作式帐神技术安全 X1300-X1399 对作式帐神技术安全 X1300-X1399 对作式帐神技术安全 X1300-X1399 对作式帐神技术安全 X1300-X1399 X1300-X1399 X1300-X1399 为信式帐神技术安全 X1300-X1399 对信或性的大量全 X1300-X1399 对信或性的大量全 X1300-X1399 对信或性的大量全 X1300-X1399 对信或性的大量全 X1300-X1399 对信或性的大量全 X1300-X1399 X1500-X1519 漏洞状态信息交换 事件中故启发或信息交换 事件中故启发或信息交换 事件的或数 X1500-X1519 高温积虚色的关系 X1500-X1559 系11位 X1500-X1559 系11位 X1500-X1559 系11位 X1600-X1659 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1559 X1500-X1590 X1500-X1601 X1500-X1601 X1600-X1610 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1619 X1600-X1629 X1600-X1639 X1700-X1711 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1721 X1710-X1729 X1710-X1729 X1720-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1729 X1730-X1728 X1730-X1729 X1730-X1730 X1730-X1730 X1730-X1730 X1730-X1730 X1730-X1730 X1730-		
生物測定 X.1080-X.1099 安全应用和服务 (1) X.1100-X.1109 解庭网络安全 X.1110-X.1139 阿安全 X.1140-X.1139 阿安全 X.1140-X.1149 安全协议 (1) X.1150-X.1159 对等网络安全 X.1160-X.1169 网络身份安全 X.1160-X.1179 PPTV安全 X.1180-X.1179 网络安全 X.1200-X.1229 反垃圾信息 X.1230-X.1279 安全应用和服务 (2) 应急通信 这在传感器网络安全 X.1310-X.1319 對能电网安全 X.1310-X.1319 對能电网安全 X.1310-X.1319 對能电网安全 X.1310-X.1319 對能中风安全 X.1300-X.1339 对能政域状态 X.1360-X.1369 智能交通感域大会全 X.1360-X.1369 智能交通感域大会全 X.1360-X.1369 智能交通感域大会全 X.1400-X.1369 对路域大会全 X.1400-X.1439 网络安全信息交换 X.1500-X.1519 湖海水流流信息交换 X.1500-X.1519 湖海水流流信息交换 X.1500-X.1539 海岸安全 X.1500-X.1559 成品交及会 X.1500-X.1559 成品交及会 X.1500-X.1601 太计等安全 X.1600-X.1601 <		
安全府和服务 (1) X.1100-X.1109 家庭网络安全 X.1110-X.1119 移动安全 X.1140-X.1149 安全协议 (1) X.1150-X.1159 对等网络安全 X.1160-X.1169 网络安全 X.1170-X.1179 IPITV安全 X.1180-X.1199 网络安全 X.1200-X.1229 反垃圾信息 X.1230-X.1219 安全应用和服务 (2) 应急通信 运在传感器网络安全 X.1310-X.1319 剪能电图安全 X.1310-X.1319 验证邮件 X.1300-X.1309 考能电图安全 X.1340-X.1349 物联网 (107) 安全 X.1340-X.1349 物联网 (107) 安全 X.1340-X.1349 有能、以下级人系统(ITS) X.1370-X.1389 分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1400-X.1459 网络安全信息交换 X.1500-X.1519 遍洲状态信息交换 X.1500-X.1519 遍洲状态信息交换 X.1500-X.1539 海洋安全機逐 X.1500-X.159 本计算安全機逐 X.1500-X.159 太计算安全機 X.1500-X.159 太计算安全機 X.1500-X.1601 太计算安全 X.1500-X.1601 太计算安全 X.1		
#描奏全 X.1100-X.1119 家庭网络安全 X.1110-X.1119 移动安全 X.1110-X.1119 移动安全 X.1140-X.1139 网页安全 X.1140-X.1149 Y.1140-X.1159 对等网络安全 X.1140-X.1159 对等网络安全 X.1160-X.1159 对等网络安全 X.1160-X.1159 PTV安全 X.1170-X.1179 PTV安全 X.1180-X.1199 PTV安全 X.1180-X.1199 PTV安全 X.1230-X.1229 反垃圾信息 X.1230-X.1229 安全应用和服务(2) 应急通信 X.1230-X.1230 Y.1250-X.1309 营能电网安全 X.1310-X.1319 智能电网安全 X.1310-X.1319 智能电网安全 X.1310-X.1319 智能电网安全 X.1300-X.1309 营能空通系统(ITS)安全 X.1340-X.1349 PT X.1300-X.1349 PT X.1300-X.1359 PT X.1300-X.1359 PT X.1300-X.1359 Y.1300-X.1359 Y.1300		A.1000–A.1077
家庭网络安全 X.1110-X.1119 移动安全 X.1120-X.1139 网页安全 X.1140-X.1149 安全协议(1) X.1150-X.1159 对等网络安全 X.1170-X.1179 网络字位安全 X.1170-X.1179 网络字位安全 X.1170-X.1179 网络空间安全 X.1200-X.1229 网络安全 X.1200-X.1229 反垃圾信息 X.1230-X.1249 身份管理 X.1250-X.1279 安全应用和服务(2) X.1300-X.1309 泛在传感器网络安全 X.1310-X.1319 验证邮件 X.1300-X.1309 逆证邮件 X.1300-X.1309 参问联网(IoT)安全 X.1310-X.1319 验证邮件 X.1340-X.1349 为布式账簿技术安全 X.1310-X.1389 为布式账簿技术安全 X.1310-X.1389 分布式账簿技术安全 X.1400-X.1429 安全的议(2) X.1450-X.1459 网络安全信息交换 X.1500-X.1519 漏洞状态信息交换 X.1500-X.1519 漏洞状态信息交换 X.1500-X.1519 漏洞状态信息交换 X.1500-X.1519 高滑状态信息交换 X.1500-X.1519 高滑状态信息方术 X.1500-X.1519 高滑状态信息方术 X.1500-X.1519 高滑状态信息方术 X.1500-X.1519 高滑文全全保述 X.1500-X.1519 高清的交换 X.1550-X.1559 正计算安全使进 X.1500-X.1559 正计算安全表验 X.1500-X.1569 云计算安全是健做法和指导原则 X.1500-X.1569 云计算安全是健做法和指导原则 X.1600-X.1601 云计算安全是健做法和指导原则 X.1600-X.1609 量子通信 术语 X.1700-X.1701 属于随机数发生器 X.1700-X.1701 QKDN安全技术 X.1700-X.1701 QKDN安全技术 X.1710-X.1711 QKDN安全技术 X.1710-X.1711 QKDN安全技术 X.1710-X.1719 QKDN安全技术 X.1710-X.17159		Y 1100 Y 1100
移动安全		
関页安全 安全协议 (1) 対		
安全协议(1) 对等网络安全 X.1160-X.1169 网络身份安全 X.1170-X.1179 IPTV安全 网络空间安全 网络安全 反垃圾信息 身份管理 X.1230-X.1249 身份管理 这定任德郡陽外安全 X.1300-X.1309 这在传感器网络安全 X.1310-X.1319 智能电网安全 X.1330 X.1319 智能电网安全 X.1330 X.1339 验证邮件 X.1330 X.1339 物联网(IoT)安全 X.1340-X.1349 物联网(IoT)安全 X.1340-X.1349 物联网(IoT)安全 X.1340-X.1349 物联网(IoT)安全 X.1340-X.1349 和大张青技术安全 X.1370-X.1389 为有式账簿技术安全 X.1370-X.1389 对有式账簿技术安全 X.1400-X.1519 漏洞状态信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1520-X.1519 漏洞状态信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1520-X.1559 启发式和信息时录 X.1520-X.1559 启发式和信息时录 X.1520-X.1559 后发式和信息时录 X.1520-X.1559 后发式和信息时录 X.1520-X.1559 后发式和信息时录 X.1520-X.1559 后发式和信息时录 X.1520-X.1559 和发生便量性微达和指导原则 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 云计算安全慢计 X.1520-X.1559 五计算安全慢性微达和指导原则 X.1620-X.1601 云计算安全慢性微达和指导原则 X.1620-X.1639 式计算安全量性微达和指导原则 X.1620-X.1639 式计算公主是目的机数发生器 X.1720-X.1701 QKDN安全性误 X.1710-X.1711 QKDN安全技术 X.1720-X.1729 数据安全 大数据安全		
対等网络安全 X.1160-X.1169		
网络身份安全		
IPTV安全		
网络空间安全		
网络安全		A.1100–A.117)
反迫 規信息		X 1200_X 1229
身份管理 X.1250—X.1279 安全应用和服务(2) X.1300—X.1309 泛在传感器网络安全 X.1310—X.1319 菊能电网安全 X.1340—X.1349 物联网(IoT)安全 X.1360—X.1369 智能交通系统(ITS)安全 X.1400—X.1438 分布式账簿技术安全 X.1430—X.1449 安全协议(2) X.1450—X.1459 网络安全概述 X.1500—X.1519 漏洞/状态信息交换 X.1520—X.1539 事件/事故/启发式信息交换 X.1500—X.1519 政策的交换 X.1550—X.1559 启发式和信息请求 X.1500—X.159 标识和发现 X.1560—X.159 本市外政规 X.1500—X.159 本市外政规 X.1500—X.159 本市外政规 X.1500—X.159 本市外政规 X.1500—X.159 本市等安全概述 X.1500—X.159 云计算安全最佳做法和指导原则 X.1600—X.1639 云计算安全最佳做法和指导原则 X.1600—X.169 量子通信 X.1600—X.169 本语 X.1700—X.1701 量子随机数发生器 X.1710—X.1711 QKDN安全提供 X.1710—X.1711 QKDN安全设计 X.1720—X.1729 数据安全 X.1750—X.1759		
安全应用和服务 (2) 应急通信 X.1300~X.1309 泛在传感器网络安全 X.1310~X.1319 智能电网安全 X.1330~X.1339 验证邮件 X.1340~X.1349 物联网 (IoT) 安全 X.1340~X.1349 物联网 (IoT) 安全 X.1370~X.1389 分布式账簿技术安全 X.1400~X.1429 分布式账簿技术安全 X.1430~X.1449 安全协议 (2) X.1450~X.1459 网络安全信息交换 X.1500~X.1519 漏洞状态信息交换 X.1500~X.1519 漏洞状态信息交换 X.1500~X.1519 减弱状态信息交换 X.1540~X.1549 政策的交换 X.1540~X.1559 X.1560~X.1559 启发式和信息请求 X.1500~X.1559 X.1500~X.1559 标识和是现现 X.1570~X.1579 X.1580~X.1589 云计算安全 X.1500~X.1601 X.1500~X.1601 云计算安全设计 X.1600~X.1601 X.1602~X.1639 云计算安全实施方案 X.1600~X.1679 X.1600~X.1679 量子通信 X.1700~X.1701 量子随机数发生器 X.1700~X.1701 量子随机数发生器 X.1710~X.1711 QKDN安全被表 X.1710~X.1711 QKDN安全设计 X.1710~X.1711 X.1710~X.1719 QKDN安全设计 X.1720~X.1729 数据安全 X.1750~X.1759		
应急通信		A.1230 A.127)
※ ※ ※ ※ ※ ※ ※ ※ ※ ※		X 1300-X 1309
響能电网安全 いいます。 いいます。 いいます。 いいます。 対います。 はいます。 はい		
 验证邮件 物联网 (IoT) 安全 知式360-X.1369 智能交通系统 (ITS) 安全 次1.370-X.1389 分布式账簿技术安全 次1400-X.1429 分布式账簿技术安全 次1.440-X.1449 安全协议 (2) 网络安全信息交换 网络安全概述 X.1500-X.1519 漏洞/状态信息交换 政策的交换 启发式和信息请求 水.1560-X.1559 启发式和信息请求 X.1560-X.1559 标识和发现 城保交换 云计算安全 云计算安全投计 云计算安全投计 云计算安全投计 云计算安全投计 云计算安全设计 云计算安全表建做法和指导原则 式.1600-X.1601 云计算安全交施方案 其.1660-X.1659 对.1660-X.1659 量子通信 术语 水.1600-X.1701 量子随机数发生器 QKDN安全框架 QKDN安全框架 QKDN安全技术 X.1710-X.1711 QKDN安全技术 X.1720-X.1729 数据安全 大数据安全 		
物联网 (IoT) 安全 X.1360-X.1369 智能交通系统 (ITS) 安全 X.1370-X.1389 分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1430-X.1449 安全协议 (2) X.1450-X.1459 网络安全信息交换 X.1500-X.1519 屬洞/状态信息交换 X.1520-X.1539 事件事故启发式信息交换 X.1540-X.1549 政策的交换 X.1550-X.1559 局发式和信息请求 X.1500-X.1569 标识和发现 X.1570-X.1579 确保交换 X.1580-X.1589 云计算安全 X.1500-X.1601 云计算安全设计 X.1600-X.1601 云计算安全设计 X.1600-X.1639 云计算安全实施方案 X.1600-X.1639 其他云计算安全 X.1600-X.1679 其他云计算安全 X.1600-X.1699 量子随信 X.1700-X.1701 量子随机数发生器 X.1700-X.1701 QKDN安全框架 X.1710-X.1711 QKDN安全技术 X.1710-X.1711 QKDN安全技术 X.1712-X.1719 XM安全 X.1750-X.1759		
智能交通系统 (ITS) 安全 X.1370-X.1389 分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1430-X.1449 安全协议 (2) X.1450-X.1459 网络安全信息交换 X.1500-X.1519 漏洞/状态信息交换 X.1500-X.1519 漏洞/状态信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1550-X.1559 启发式和信息请求 X.1560-X.1559 启发式和信息请求 X.1560-X.1559 后发式和信息请求 X.1560-X.1559 云计算安全 X.1570-X.1579 确保交换 X.1570-X.1579 证保交换 X.1580-X.1589 云计算安全设计 X.1600-X.1601 云计算安全设计 X.1602-X.1639 云计算安全设计 X.1640-X.1659 云计算安全设计 X.1640-X.1659 其中运计算安全 X.1660-X.1679 其中运计算安全 X.1680-X.1699 量子通信 X.1700-X.1701 量子随机数发生器 X.1700-X.1701 Q.KDN安全投计 X.1710-X.1711 Q.KDN安全投计 X.1710-X.1711 Q.KDN安全投计 X.1712-X.1719 Q.KDN安全技术 X.1710-X.1719 数据安全 大数据安全 X.1750-X.1759		
分布式账簿技术安全 X.1400-X.1429 分布式账簿技术安全 X.1430-X.1449 安全协议 (2) X.1450-X.1459 网络安全概述 X.1500-X.1519 漏洞/状态信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1540-X.1549 政策的交换 X.1550-X.1559 启发式和信息请求 X.1560-X.1569 标识和发现 X.1570-X.1579 确保交换 X.1580-X.1589 云计算安全 X.1600-X.1601 云计算安全概述 X.1600-X.1601 云计算安全设计 X.1602-X.1639 云计算安全最佳做法和指导原则 X.1600-X.1679 其他云计算安全 X.1680-X.1699 量子通信 X.1700-X.1701 量子随机数发生器 X.1700-X.1701 QKDN安全提供 X.1710-X.1711 QKDN安全提供 X.1710-X.1711 QKDN安全提供 X.1712-X.1719 QKDN安全技术 X.1720-X.1729 数据安全 X.1750-X.1759		
分布式账簿技术安全 X.1430-X.1449 安全协议(2) X.1450-X.1459 网络安全信息交換 X.1500-X.1519 漏洞/状态信息交换 X.1520-X.1539 事件/事故/启发式信息交换 X.1540-X.1549 政策的交换 X.1550-X.1559 启发式和信息请求 X.1560-X.1569 标识和发现 X.1570-X.1579 确保交换 X.1580-X.1589 云计算安全 X.1600-X.1601 云计算安全模量 X.1602-X.1639 云计算安全是健做法和指导原则 X.1640-X.1659 云计算安全实施方案 X.1660-X.1679 其他云计算安全 X.1680-X.1699 量子通信 X.1700-X.1701 量子随机数发生器 X.1710-X.1711 QKDN安全提架 X.1710-X.1711 QKDN安全设计 X.1710-X.1711 QKDN安全设计 X.1710-X.1719 QKDN安全设计 X.1720-X.1729 数据安全 X.1750-X.1759		
安全协议 (2)X.1450-X.1459网络安全信息交換X.1500-X.1519漏洞/状态信息交換X.1520-X.1539事件/事故/启发式信息交换X.1540-X.1549政策的交换X.1550-X.1559启发式和信息请求X.1570-X.1579标保交换X.1580-X.1589云计算安全X.1580-X.1589云计算安全概述X.1600-X.1601云计算安全身健做法和指导原则X.1640-X.1659云计算安全实施方案X.1660-X.1679其他云计算安全X.1680-X.1699量子通信X.1700-X.1701水语X.1700-X.1701量子随机数发生器X.1710-X.1711QKDN安全程架X.1710-X.1711QKDN安全设计X.1710-X.1712QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759		
网络安全信息交換		
网络安全概述		
漏洞/状态信息交换 事件/事故/启发式信息交换 政策的交换 以1540-X.1549 政策的交换 以1550-X.1559 启发式和信息请求 以1560-X.1569 标识和发现 X.1570-X.1579 确保交换 X.1580-X.1589 云计算安全 云计算安全概述 云计算安全设计 云计算安全最佳做法和指导原则 云计算安全或计算安全或计算安全或计算安全或计算安全或计算安全或计算安全或计算安全或		X.1500-X.1519
事件/事故/启发式信息交换X.1540-X.1549政策的交换X.1550-X.1559启发式和信息请求X.1560-X.1569标识和发现X.1570-X.1579确保交换X.1580-X.1589云计算安全X.1600-X.1601云计算安全设计X.1602-X.1639云计算安全最佳做法和指导原则X.1640-X.1659云计算安全实施方案X.1660-X.1679其他云计算安全X.1680-X.1699量子通信X.1700-X.1701本语X.1700-X.1701夏子随机数发生器X.1702-X.1709QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759		
政策的交換 启发式和信息请求 标识和发现 		
启发式和信息请求 X.1560—X.1569 标识和发现 X.1570—X.1579 确保交换 X.1580—X.1589 X.1580—X.1589 X.159全 X.1580—X.1589 X.159		
标识和发现 确保交换X.1570-X.1579云计算安全 云计算安全概述 云计算安全设计 云计算安全最佳做法和指导原则 云计算安全实施方案 其他云计算安全 里子通信 水語 水語 型子通信 水語 型子随机数发生器 QKDN安全框架 QKDN安全设计 QKDN安全设计 QKDN安全技术 数据安全 大数据安全X.1500-X.1701 X.1710-X.1711 X.1712-X.1719 X.1712-X.1719 X.1720-X.1729		
确保交換 云计算安全 云计算安全概述 云计算安全设计 云计算安全设计 云计算安全最佳做法和指导原则 云计算安全实施方案 其他云计算安全 工1660-X.1679 其他云计算安全 里子通信 水语 水语 不语 子の 人の <td></td> <td></td>		
云计算安全X.1600-X.1601云计算安全设计X.1602-X.1639云计算安全最佳做法和指导原则X.1640-X.1659云计算安全实施方案X.1660-X.1679其他云计算安全X.1680-X.1699量子通信X.1700-X.1701最子随机数发生器X.1702-X.1709QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全大数据安全大数据安全X.1750-X.1759		
云计算安全概述X.1600-X.1601云计算安全设计X.1602-X.1639云计算安全最佳做法和指导原则X.1640-X.1659云计算安全实施方案X.1660-X.1679其他云计算安全X.1680-X.1699量子通信X.1700-X.1701量子随机数发生器X.1702-X.1709QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759		
云计算安全设计 云计算安全最佳做法和指导原则 云计算安全实施方案 其他云计算安全 		X.1600-X.1601
云计算安全最佳做法和指导原则X.1640-X.1659云计算安全实施方案X.1660-X.1679其他云计算安全X.1680-X.1699量子通信X.1700-X.1701术语X.1702-X.1709QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759		
云计算安全实施方案 其他云计算安全X.1660-X.1679 X.1680-X.1699量子通信 术语 量子随机数发生器 QKDN安全框架 QKDN安全设计 QKDN安全设计 QKDN安全技术 数据安全 大数据安全X.1700-X.1701 X.1710-X.1711 X.1712-X.1719 X.1720-X.1729		
其他云计算安全 量子通信 术语 X.1700—X.1701 量子随机数发生器 X.1702—X.1709 QKDN安全框架 X.1710—X.1711 QKDN安全设计 X.1712—X.1719 QKDN安全技术 X.1720—X.1729 数据安全 大数据安全		
量子通信 术语		
术语X.1700-X.1701量子随机数发生器X.1702-X.1709QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759		
量子随机数发生器X.1702–X.1709QKDN安全框架X.1710–X.1711QKDN安全设计X.1712–X.1719QKDN安全技术X.1720–X.1729数据安全X.1750–X.1759		X.1700-X.1701
QKDN安全框架X.1710-X.1711QKDN安全设计X.1712-X.1719QKDN安全技术X.1720-X.1729数据安全X.1750-X.1759	, ···	
QKDN安全设计 X.1712–X.1719 QKDN安全技术 X.1720–X.1729 数据安全 X.1750–X.1759		
QKDN安全技术 X.1720–X.1729 数据安全 X.1750–X.1759		
数据安全 大数据安全 X.1750–X.1759		
大数据安全 X.1750-X.1759		
		X.1750-X.1759
	5G 安全	X.1800-X.1819

ITU-T X.1367 建议书

物联网(IoT)安全事件操作的错误日志标准格式

摘要

在处理来自物联网(IoT)生态系统的安全事件方面存在两个问题:第一个是使用传输控制协议/互联网协议(TCP/IP)的计算机网络与物联网边缘设备之间的协议不兼容。第二是边缘设备制造商之间的错误代码缺乏兼容性。

X.1367建议书规定一种标准化的、可置于协议有效载荷中的错误日志格式(见IETF RFC 5424),用于将边缘设备发出的错误日志信息转换为标准的错误日志格式。

本建议书还对标准化的错误代码表做出规定以解决第二个问题。因此,可以对计算机网络和物联网边缘设备网络之间的安全事件进行整合管理。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1367	2020-09-03	17	11.1002/1000/14263

关键词

边缘设备、错误代码、错误日志格式、事件响应、物联网(IoT)、安全操作

^{*} 欲查阅建议书,请在您的网络浏览器地址域键入URL http://handle.itu.int/,随后输入建议书的唯一ID,例如,http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟(ITU)是从事电信、信息和通信技术(ICT)领域工作的联合国专门机构。国际电信联盟电信标准化部门(ITU-T)是国际电信联盟的常设机构,负责研究技术、操作和资费问题,并且为在世界范围内实现电信标准化,发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会(WTSA)确定ITU-T各研究组的研究课题,再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准,是与国际标准化组织(ISO)和国际电工技术委员会(IEC)合作制定的。

注

本建议书为简明扼要起见而使用的"主管部门"一词,既指电信主管部门,又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的,但建议书可能包含某些强制性条款(以确保例如互操作性或适用性等),只有满足所有强制性条款的规定,才能达到遵守建议书的目的。"应该"或"必须"等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意:本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止,国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是,这可能并非最新信息,因此大力提倡他们通过下列网址查询电信标准化局(TSB)的专利数据库: http://www.itu.int/ITU-T/ipr/.。

© 国际电联 2021

版权所有。未经国际电联事先书面许可,不得以任何手段复制本出版物的任何部分。

目录

			页码
1	范围		1
2	参考文	T献	1
3	定义		1
	3.1	他处定义的术语	1
	3.2	本建议书中定义的术语	2
4	缩写词]和首字母缩略语	2
5	惯例		3
6	总论		3
	6.1	物联网生态系统中的当前错误处理	3
	6.2	概述	4
7	物联网]环境的标准错误日志格式	4
	7.1	错误日志格式的基本结构	4
	7.2	基本属性	5
附件A	A – 错误	代码和错误消息	6
附录-	一—如何	可将错误日志用于事件操作的示例	7
	I.1	攻击者通过IoTGW向边缘设备发送随机二进制字符串	7
	I.2	攻击者通过受损的IoTGW向边缘设备发送不正确的认证	8
	I.3	攻击者实际破坏无需任何请求而定期发送数据的传感器设备	9
	I.4	如何在事件响应中使用物联网日志	9
附录二	二-使月	引物联网错误日志的预期安全事件响应	12
参老丰			13

ITU-T X.1367 建议书

物联网(IoT)安全事件操作的错误日志标准格式

1 范围

本建议书规定一种标准化的、可置于协议有效载荷中的错误日志格式(例如syslog [b-IETF RFC 5424]),用于将边缘设备发出的错误日志信息转换为标准的错误日志格式。

本建议书还规定了一个标准化的错误代码表,以解决边缘设备制造商之间错误代码不兼容的问题。因此,可以对计算机网络和物联网边缘设备网络之间的安全事件进行整合管理。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书使用以下其它地方定义的术语:

- **3.1.1** 执行器 (actuator) [ITU-T Y.4109]: 在输入信号刺激后触发物理行动的设备。
- **3.1.2** 攻击(attack)[b-ISO13491-1]: 对手为获取或修改敏感信息或未被授权获取或修改的服务而对设备发起的进攻尝试。
- **3.1.3 身份验证(authentication)**[b-ITU-T X.1277]: 身份验证是用户使用其 FIDO 验证符向依赖方证明拥有注册密钥的过程。
- **3.1.4 授权 (authorization)** [b-ITU-T X.800]: 权利的授予,包括根据访问权准予访问。
- **3.1.5 设备(device)** [b-ITU-T Y.4000]: 在物联网中,具有强制性通信能力和选择性传感、激励、数据捕获、数据存储和数据处理能力的设备。
- **3.1.6 物联网(Internet of Things)(IoT)**[b-ITU-T Y.4000]: 信息社会的一种全球基础设施,基于现有的和正在出现的、可互操作的信息和通信技术,实现(物理和虚拟)之物的相互连接,以提供先进的服务。
- **3.1.7 人/机接口(human/machine interface)(HMI)**[b-ITU-T H.320]: 用户和终端/系统之间的人机接口,由物理部分(电声、电光转换器、按键等)和处理功能操作状态的逻辑部分组成。
- **3.1.8 恶意软件(malware)**[b-ISO/IEC 27033-1]: 旨在专门破坏或干扰系统,攻击其保密性、完整性与/或可用性的怀有恶意的软件。
- **3.1.9 传感器(sensor**)[ITU-T Y.4105]: 传感物理条件或化合物并传递与所观测到的特性相关的电子信号的电子设备。
- **3.1.10 物 (thing)** [b-ITU-T Y.4000]: 在物联网中, "物"指物理世界(物理事物)或信息世界(虚拟事物)中的一个对象,它可被标识并整合进通信网络中。

3.1.11 漏洞(vulnerability)[b-ISO/IEC 27000]: 可能被一个或多个威胁利用的资产或控制的薄弱之处。

3.2 本建议书中定义的术语

本建议书定义了下列术语:

- **3.2.1** 认证(certification):与产品、流程、系统或人员相关的第三方证明。
- 注 基于[b- ISO/IEC 17000]中的定义。
- **3.2.2 命令与控制(C&C)服务器(command and control(C&C)server)**: 向被恶意软件感染后变成僵尸的计算机(僵尸网络)发送命令并对其进行控制的服务器。
- **3.2.3** 加密(encryption):对数据进行加密转换以产生密文。
- 注 基于[b-ITU-T X.800]中的加密(encipherment)定义,该定义将加密(encryption)视为其同义词。
- **3.2.4 物联网边缘设备(Internet of things edge device)**: 物联网生态系统的终端设备,通过传感器从现实世界收集数据,或通过执行器影响现实世界。
- **3.2.5 物联网网关(Internet of things gateway(IoTGW))**: 连接物联网边缘设备网络和广泛可用的计算机网络(如互联网)的设备。
- **3.2.6 微控制器单元(microcontroller unit(MCU)):** 一种嵌入式微处理器,将算法单元、存储单元和输入/输出端口集成到一个集成电路中。
- **3.2.7** 安全事件响应团队(security incident response team(SIRT)):接收、调查和响应"安全事件"报告的团队。
- **3.2.8 安全操作中心(security operations centre(SOC))**: 监视组织中的计算机和网络状态并在发现恶意活动的迹象后做出响应的部门。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语:

C&C 命令与控制

FW 防火墙

HMI 人/机接口

ID 识别符

IDS 入侵检测系统

IoT 物联网

IoTGW 物联网网关

IP 互联网协议

JSON JavaScript对象表示法

LAN 局域网

MCU 微控制器单元

PC 个人计算机

SIRT 安全事件响应团队

SOC 安全操作中心

TCP 传输控制协议

5 惯例

无。

6 总论

6.1 物联网生态系统中的当前错误处理

在物联网错误处理环境中,如果物联网系统中的某个组件(如传感器或执行器)出现故障,则发出错误代码并记录在错误日志中。如果错误很少发生,则不需要纠正。但是,如果错误持续发生,则应更换组件,以解决问题。

图 1 显示由物联网组件组成的典型物联网生态系统,包括与传感器和执行器相关联的微控制器单元(MCU)、物联网网关(IoTGW)和云。

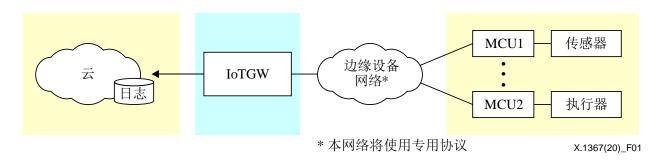


图 1 - 典型物联网生态系统

图1中的IoTGW、MCU1和MCU2之间的通信基于系统的专用协议(参见注)。MCU1传感器和MCU2执行器是物联网边缘设备示例。在这种情况下,IoTGW向MCU发送请求,MCU用日志信息回应IoTGW。IoTGW还与云(后台系统)通信。

注 – 专用协议可以是用于大型网络的协议,如oneM2M [b-oneM2M]、ECHONET Lite [b-ISO/IEC 14543-4-3],也可以是用于小型网络的协议,如SPI [b-SPI]、 I^2 C [b-UM10204]、蓝牙[b-IEEE 802.15.1]、紫蜂(Zigbee)[b-IEEE 802.15.4],或者是专为此物联网系统设计的专有协议。

为了适当管理物联网生态系统,因为物联网边缘设备有时会发生故障,所以物联网生态系统需要处理错误。这种系统处理带有错误代码的错误日志并启动修复。另一方面,一些系统会分析存储有错误代码的错误日志,以整理统计信息来改进自身,甚至处理安全事件。然而,很难统一每个物联网生态系统和系统日志的错误日志[b-IETF RFC 5424]。

6.2 概述

为了有效应对事件,提供从物联网生态系统组件收集和分析错误日志信息的足够能力至 关重要。然而,在物联网生态系统情况下,我们认识到存在以下问题。

- 1) 有标准化程序,包括通过使用系统日志的事件处理流程[b-IETF RFC 5424],以便从 网络设备收集日志信息。然而,物联网生态系统却不具备这样的程序。
- 2) IoT 错误日志信息不能存储在 IoT 生态系统的单个组件中,即此类日志信息应由后台系统(如云)或 IoT 边缘系统(如 IoTGW)收集,具体取决于 IoT 生态系统的配置。
- 3) 不同物联网组件之间的错误日志信息的相关性分析很困难,因为没有标准化的错误日志格式。
- 4) 如果没有处理错误日志信息的方法,物联网生态系统将无法有效维护其物联网服务。

本建议书建议描述用于在事件处理操作中收集物联网错误日志的基本物联网系统架构。 建议书具体规定标准化错误代码和错误日志格式。通过将每个物联网生态系统制造商采用的 错误代码转换为标准化错误代码,可以更有效地监控多个物联网生态系统的状态。此外,在 将错误代码转换为标准化错误代码的过程中,发生错误的情况也记录在相关的错误日志中。 因此,可以跨多个物联网生态系统处理安全事件。(参见附录一第I.4节 – 多物联网生态系统 中的示例)

7 物联网环境的标准错误日志格式

由于计算机资源不足,所以物联网边缘设备很难实施处理物联网错误日志的新功能。然而,IoTGW通常有更好的计算机资源来做到这一点。请求和回应通常在IoTGW和云系统之间交换,且此类通信包括物联网错误日志信息。因此,本建议书要求IoTGW生成标准化错误日志信息,并将其传达给云系统。

7.1 错误日志格式的基本结构

物联网错误日志使用带有正则表达式的JavaScript对象表示法(JSON),其格式如图2所示。这种格式可以转换为系统日志或XML格式(参见注)。附录一描述这种格式的示例。 注 - 本建议书没有定义每个属性值的长度。错误日志的发送方和接收方需要事先就每个属性值的长度达成一致。

```
{
   "Timestamp":
         "^{(0-9)}{4}) - (1[0-2]|0[1-9]) - (3[01]|0[1-9]|[12][0-9])T
           (2[0-3],[01],[0-9]):([0-5],[0-9]):([0-5],[0-9],(\.,[0-9],\{+\}),\mathbb{Z}^*,
  "Reporter":
                                                                                    { },
  "Protocol":
                                                                                String,
  "Requester":
                                                                                    { },
  "Responder":
                                                                                    { } ,
  "Error
                                  Code":
                                                                  "/^[0-9A-F]^{+}$/",
  "Error
                                       Message":
                                                                                String,
  "Description":
                                      String
                                                                { },
}
```

图 2 - 错误记录要素

大多数情况下,该错误日志的报告方是IoTGW。该格式中使用的属性在第7.2节中得到定义。

7.2 基本属性

以下属性是错误日志信息的组成要素。

- a) 时间标记:发出错误日志需要时间标记(见注)。例如,在2018年9月20日-13时25分51秒的情况下,时间标记应描述为"2018-09-20T13:25:51.0Z." [b-ISO 8601-1]。
- 注 "时间标记"是强制性的,即使带有本建议书规定的错误日志的传输协议也有时间标志字段,因为时间标记通常在问题发生和传送时间之间发生变化。
- b) 报告方:将设备错误代码转换为标准错误代码并将其发送到云端的物联网组件。详细描述见图 3。

图 3-报告方要素

- 1) 互联网协议(IP)地址:以太网上报告方的唯一标识符(ID)。
- c) 协议: 在 IoTGW 和物联网边缘设备之间使用的协议名称。
- d) 请求方或回应方: 向物联网边缘设备发送请求的物联网组件或回复请求的物联网组件。详细描述见图 4。

```
"Requester(or Responder)": {
    "Unique ID": string,
    "Transmitted Code": "([0-9A-F])^{+}}
```

图 4 - 请求方和回应方要素

- 1) 唯一ID(可选): 这是与物联网边缘设备网络协议定义的每个设备相关的唯一编号或唯一代码。
- 2) 传输代码(可选):传输数据的内容,用十六位表示。
- 3) 在没有请求方或回应方的情况下发生错误时,应如图 5 所示,就像传感器设备在没有请求的情况下周期性地发送数据一样。

```
"Requester(or Responder)": {}
```

图 5 - 没有请求方或没有回应方的情况

- e) 错误代码、错误消息:错误代码和错误消息在附录 A 中规定。
- f) 说明(可选):如果需要通知物联网边缘设备或其网络的情况,可以表达 JSON 的任何句子、短语和子元素。

如果通信带宽较窄或存储空间有限,可以省略错误消息。如果没有必要写任何附加文本,则可以省略说明。

附件 A

错误代码和错误消息

(此附件为本建议书不可分割的组成部分)

错误代码和错误消息在表A.1中具体规定。

表 A.1 - 错误代码和错误消息

代码	消息	说明		
	无误码(0x00-0x0F)			
0x00	无误码	无误码出现。		
	通信(0x10-0x1F)			
0x10	无回应	即使请求要求回应也没有响应。		
0x11	通信失败	通信失败的若干问题。		
0x12	链路断开	网络接口链接断开。		
0x1E	扩展原因	扩展原因的前缀代码。		
0x1F	其他通信原因	与通信有关的其他原因。		
	安全(0x20-0x2F)			
0x20	验证失败	验证的若干问题。		
0x21	认证失败	认证的若干问题。		
0x22	加密失败	加密的若干问题。		
0x23	授权失败	授权的若干问题。		
0x2E	扩展原因	扩展原因的前缀代码。		
0x2F	其他安全原因	与验证、认证、加密或授权有关的其他原因。		
	命令 (0x30-0x3F)			
0x30	无效命令	命令未定义或无效。		
0x31	非法参数	参数超出范围或无效。		
0x3E	扩展原因	扩展原因的前缀代码。		
0x3F	其他命令原因	与命令相关的其他原因。		
	设备(0x40-0x4F)			
0x40	设备损坏	设备的一部分已损坏,无法修复。		
0x41	设备故障	设备的一部分出现故障,但可恢复。		
0x42	资源不足	耗尽存储、内存和任何计算资源。		
0x4E	扩展原因	扩展原因的前缀代码。		
0x4F	其他设备原因	与设备相关的其他原因。		
	预留用于未来扩展(0x5			
	预留用于私人应用(0xI	CO-OxEF)		
	其他(0xF0-0xFF)			
0xFF	其他原因	除上述原因外的其他原因。		

附录一

如何将错误日志用于事件操作的示例

(此附录非本建议书不可分割的组成部分)

I.1 攻击者通过 IoTGW 向边缘设备发送随机二进制字符串

图I.1显示攻击者向MCU1发送随机二进制字符串及后者的反应。随机二进制字符串"01000001"的字头标识0001号设备和0100号功能。换句话说,攻击者试图攻击0001号设备的0100号功能。MCU1无法理解"3A459187F43CDDE5",因此,它用"000003FF(未知命令)"向0000号设备(IoTGW)做出回应。

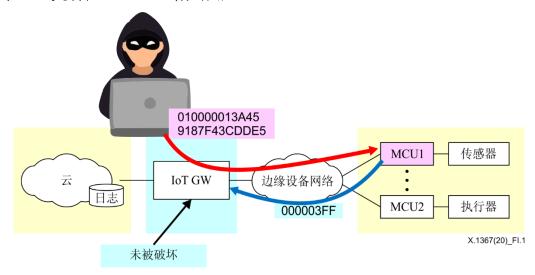


图 I.1 - 攻击者向 MCU1 发送随机二进制字符串

在IoTGW从MCU1收到"000003FF"后,IoTGW构建以下日志并将其发送到云中的日志服务器。见图I.2。

```
{
   "Timestamp": "2018-08-28T09:34:55.0Z",
                         "IP
   "Reporter":
                                          Address":
                                                            "192.168.2.11"},
                      {
                            "ABC
   "Protocol":
                                            company
                                                                  protocol",
   "Requester":
                                                                     "0000",
                                        ID":
       "Unique
        "Transmitted
                               Code":
                                                  "010000013A459187F43CdDE5"
   "Responder":
                                                                     "0001",
       "Unique
                                        ID":
       "Transmitted
                                        Code":
                                                                  "000003FF"
                                                                       "30",
   "Error
                                     Code":
   "Error
                       Message":
                                             "Invalid
                                                                   Command",
}
```

图 I.2 - 错误请求的物联网错误日志 (示例)

I.2 攻击者通过受损的 IoTGW 向边缘设备发送不正确的认证

图I.3显示攻击者通过受损的IoTGW向MCU2发送不正确的认证及后者的反应。MCU2识别出认证无效,因此,以"0000010000c(证书验证错误)"向0000号设备(IoTGW)做出回应,但IoTGW已受到损害。IoTGW永远不会向云端的日志服务器发送错误日志。入侵发现系统(IDS)会发送物联网错误日志,而非IoTGW。

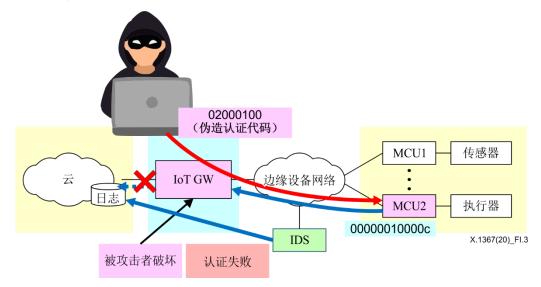


图 I.3 - 攻击者发送伪造认证代码

攻击者向MCU2发送伪造认证代码,但MCU2无法予以识别。因此,MCU2发送 "00000010000c(证书验证错误)"。IoTGW忽略来自MCU2的回应消息,因为攻击者此前已将网关损坏。然而,如果系统有IDS,则IDS会在图I.4中构建物联网错误日志,而非IoTGW。在这种情况下,IDS变为报告方。

```
"Timestamp": "2018-08-28T09:34:55.0Z",
             { "IP
"Reporter":
                                   Address":
                                                   "192.168.100.249"},
"Protocol":
                      "EEE
                                      Company's
                                                          protocol",
"Requester":
                                                               "0000",
   "Unique
                                 Name":
   "Transmitted Code": "02000100... (Faked certification codes)"
"Responder":
   "Unique
                                                               "0002",
                                 Name":
   "Transmitted
                         Code":
                                         "00000000010000c
} ,
"Error
                                                                "21",
                                Code":
"Error
                                     "Certification
                                                             Failed",
                Message":
"Description":
   "Status":
               "This
                      message
                                             from IDS not
                                                               IoTGW"
                                was
                                      sent
},
```

图 I.4 - 证书验证错误的物联网错误日志 (示例)

I.3 攻击者实际破坏无需任何请求而定期发送数据的传感器设备

图I.5显示攻击者实际破坏无需任何请求而定期发送数据的MCU1。此后,MCU1不能发送任何数据。在这种情况下,IoTGW发现与MCU1相关的异常情况,并发送图I.6所示的物联网错误日志。

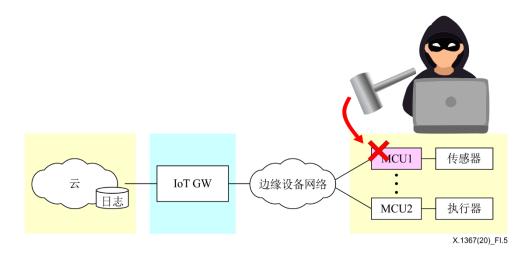


图 I.5 - 攻击者实际破坏 MCU1

```
"Timestamp":"2018-08-28T09:34:55.0Z",
   "Reporter": { "IP
                                                     "192.168.10.254"},
                                    Address":
   "Protocol":
                                        Company's
                                                            protocol",
   "Requester":
                                                                   { },
   "Responder":
                                                               "0002",
       "Unique
                                   Name":
       "Transmitted
                                        Code":
   } ,
   "Error
                                  Code":
                                                                 "11",
                                                             Failed",
                                     "Communication
   "Error
                  Message":
   "Description":
       "Responder
                         stopped
                                             sending
                                                                data."
   },
}
```

图 I.6 - 因失去通信而发送的物联网错误日志(示例)

I.4 如何在事件响应中使用物联网日志

如图I.7所示,一家工厂在同一个局域网(LAN)上有三个物联网生态系统。

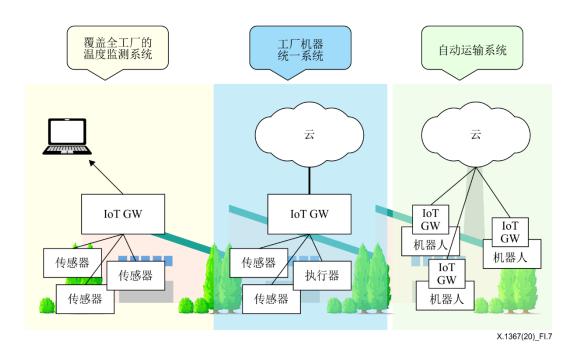


图 I.7 - 工厂中的多个物联网生态系统

如图I.8所示,在这种情况下,攻击者可轻松攻击每台设备。如果没有物联网错误日志,则安全事件响应团队(SIRT)很难识别攻击者的足迹,因为SIRT无法统一每个物联网生态系统的非标准物联网日志。

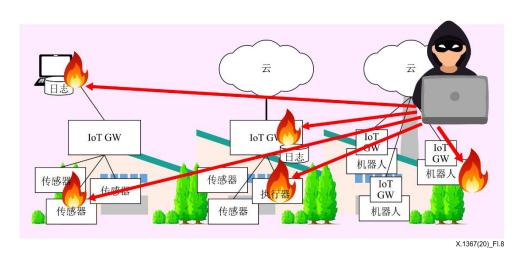


图 I.8 - 攻击者同时攻击所有物联网生态系统

如图I.9所示,如果这些物联网生态系统使用标准的物联网错误日志格式,则SIRT可以 轻而易举地统一所有的物联网错误日志以及统一系统日志。攻击者的足迹即可得到识别。

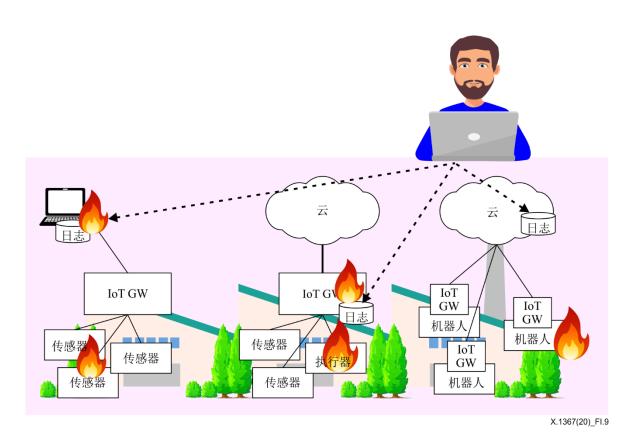


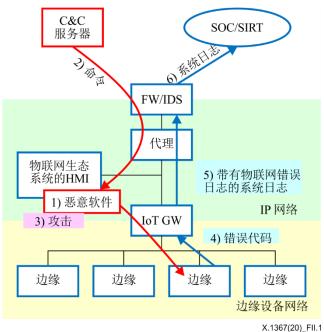
图 I.9 - 统一和分析所有物联网错误日志

附录二

使用物联网错误日志的预期安全事件响应

(此附录非本建议书不可分割的组成部分)

本建议书描述的标准物联网错误日志可用于物联网生态系统的安全事件响应。图II.1显 示使用物联网错误日志进行事件发现的流程。



图II.1 - 使用物联网错误日志进行事件发现

- 恶意软件以某种方式感染人/机接口(HMI),例如台式个人计算机(PC)。 1)
- 恶意软件从命令与控制(C&C)服务器接收命令。防火墙(FW)、IDS或代理可记 2) 录恶意软件与 C&C 服务器之间的通信日志。
- 恶意软件寻找物联网边缘设备的漏洞。物联网边缘设备向IoTGW发送许多错误代 3) 码,因为恶意软件试图频繁发送带有各种参数的命令。对于物联网边缘设备,上述 参数几乎没有正确的时候。
- 针对发送的每个物联网错误代码,IoTGW 使用系统日志协议以本建议书具体规定的 4) 格式向防火墙或 IDS 发送物联网错误日志。
- 代理亦使用系统日志协议向防火墙或 IDS 发送通信日志,前者使用系统日志协议向 5) 安全操作中心(SOC)或SIRT发送所有日志,包括物联网错误日志。

SOC或SIRT的安全分析师可能不会对与其他物联网错误日志无关的单个物联网错误日志 做出回应。然而,如果SOC或SIRT连续收到大量物联网错误日志,则他们可能会注意到出现 了异常情况,因为这可能是因为攻击者在寻找物联网系统漏洞。

本建议书允许SOC或SIRT分析师发现物联网边缘设备上的攻击,因为SOC或SIRT收到 标准物联网错误日志格式的物联网错误代码。然后,他们将检查其他相关日志,包括恶意软 件与C&C服务器之间的通信,并通知工厂操作员将该人机接口台式电脑从局域网中分离出 来,或从人机接口台式电脑中移除恶意软件。

参考书目

	多 有节日
[b-ITU-T X.800]	Recommendation ITU-T X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.
[b-ITU-T X.1277]	Recommendation ITU-T X.1277 (2018), Universal authentication framework.
[b-ITU-T Y.4000]	Recommendation ITU-T Y.4000/Y.2060 (2012), Overview of the Internet of things.
[b-ITU-T Y.4105]	Recommendation ITU-T Y.4105/Y.2221 (2010), Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.
[b-ITU-T Y.4109]	Recommendation ITU-T Y.4109/Y.2061 (2012), Requirements for the support of machine-oriented communication applications in the next generation network environment.
[b-ISO 8601-1]	ISO 8601-1:2019, Date and time – Representations for information interchange – Part 1: Basic rules.
[b-ISO 13491-1]	ISO 13491-1:2016, Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods.
[b-ISO/IEC 14543-4-3	ISO/IEC 14543-4-3:2015, Information technology – Home Electronic Systems (HES) architecture – Part 4-3: Application layer interface to lower communications layers for network enhanced control devices of HES Class 1.
[b-ISO/IEC 17000]	ISO/IEC 17000:2004, Conformity assessment – Vocabulary and general principles.
[b-ISO/IEC 27000]	ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary.
[b-ISO/IEC 27033-1]	ISO/IEC 27033-1:2015, Information technology – Security techniques – Network security – Part 1: Overview and concepts.
[b-ISO/IEC 27039]	ISO/IEC 27039:2015, Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).
[b-IEEE 802.15.1]	IEEE 802.15.1-2005, IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN).
[b-IEEE 802.15.4]	IEEE 802.15.4-2015, IEEE Standard for low-rate wireless networks.
[b-IETF RFC 5424]	IETF RFC 5424 (2009), The syslog protocol.
[b-oneM2M]	oneM2M Partners (2017), Standards for M2M and Internet of things. Available [viewed 2020-02-12] at: http://www.onem2m.org/
[b-SPI]	Motorola (2001), SPI block guide, V04.01. Available [viewed 2020-02-12] at: https://www.nxp.com/files-static/microcontrollers/doc/ref_manual/S12SPIV4.pdf
[b-UM10204]	UM10204 (2014), I^2C -bus specification and user manual, Rev.6.Available[viewed 2020-02-12] at: https://www.nxp.com/docs/en/user-guide/UM10204.pdf

ITU-T系列建议书

系列A ITU-T工作的组织

系列D 资费及结算原则和国际电信/ICT的经济和政策问题

系列E 综合网络运行、电话业务、业务运行和人为因素

系列F 非话电信业务

系列G 传输系统和媒介、数字系统和网络

系列H 视听及多媒体系统

系列I 综合业务数字网

系列J 有线网络和电视、声音节目及其他多媒体信号的传输

系列K 干扰的防护

系列L 环境与ICT、气候变化、电子废物、节能;线缆和外部设备的其他组件的建设、安装和

保护

系列M 电信管理,包括TMN和网络维护

系列N 维护: 国际声音节目和电视传输电路

系列O 测量设备的技术规范

系列P 电话传输质量、电话设施及本地线路网络

系列Q 交换和信令,以及相关的测量和测试

系列R 电报传输

系列S 电报业务终端设备

系列T 远程信息处理业务的终端设备

系列U 电报交换

系列V 电话网上的数据通信

系列X数据网、开放系统通信和安全性

系列Y 全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市

系列Z 用于电信系统的语言和一般软件问题