Security Incident Response Management

Contents

1 Security Incident Report (Level/Tier 1)

1.1 SQL Injection

1.1.1 Incident Description

Incident:	Offense 19784 : HTTP_POST_SCRIPT
Duration:	From Feb 26, 2019, 6:48:14 PM to 6:49:12 PM
Source IP(s):	172.16.11.37
Source Port(s):	53758, 51392
Target IP(s):	172.16.11.4
Target Port(s):	80
Occurrences:	4 Events 0 Flows
Severity:	9
Event Classification:	SQL injection preceded by HTTP_GET_SQL_Unionselect

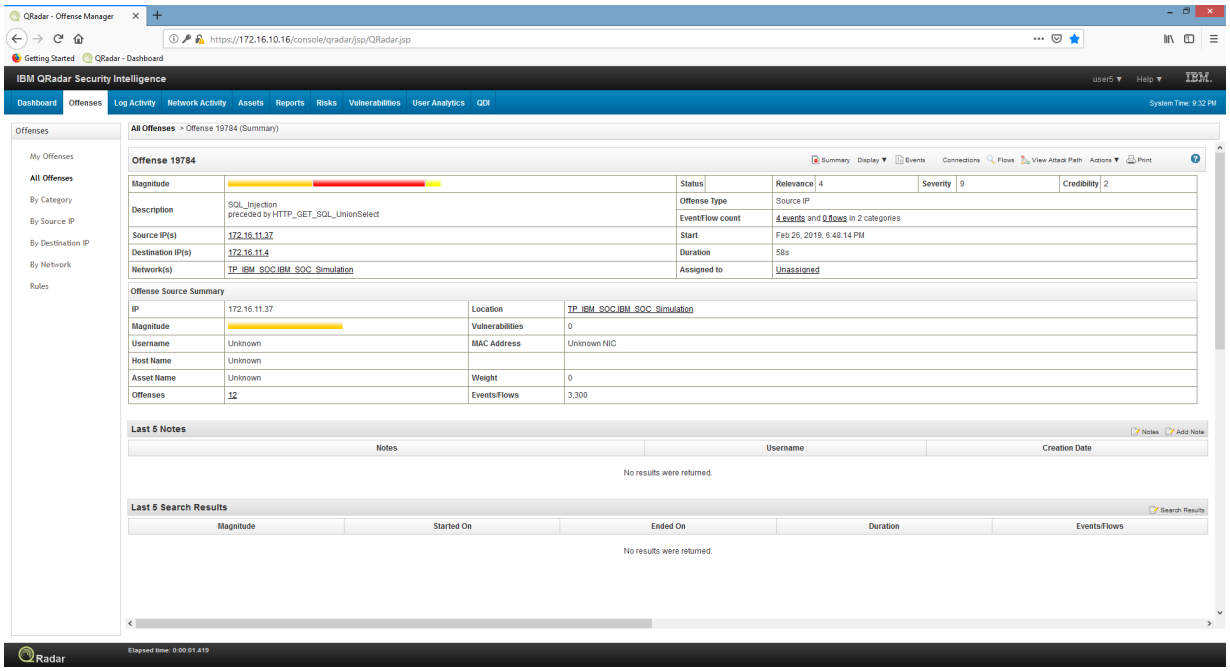
1.1.2 Threat Analysis

Examining the event logs indicated that user was attemping to perform SQL injection to query for unauthorised information from Feb 26, 2019, 6:48:14 PM to 6:49:12 PM, with the source IP "172.16.11.37" which indicated that the offense was conducted within the network of the TP. This traffic was intercepted by Bluecoat Server which had dropped the potentially malicious SQL request issued from this user. Current investigation indicated that the IP was used in the school IBM-QRADAR lab. Typically commands such as HTTP_GET_SQL_Unionselect does not necessarily indicate an attack, however it is followed by SQL injection in the context of the login page, hence the severity of the offense is 9.

1.1.3 Recommendation

This incident is escalated to TP IBM Qradar lab to identify the actual user ID by the lab server logs or checking the sign-in entries for further actions. Given that the severity of the issue is HIGH (9), it is recommended that the raw traffic packets containing exact SQL commands issued by user are to be fetched from IBM X-force database to be passed to the Tier 2 - Triage team for further analysis.

1.1.4 Supporting Data



Screen capture of Offense 19784: SQL Injection.

1.2 Cross-Site Scripting

1.2.1 Incident Description

Incident:	Offense 19777 : Cross_Site_Scripting
Duration:	0s at Feb 26, 2019, 3:30:56 PM
Source IP(s):	172.16.11.4
Source Port(s):	80
Target IP(s):	172.16.11.37
Target Port(s):	56341
Occurrences:	1 Events 0 Flows
Severity:	9
Event Classification:	Exploit; Cross_Site_Scripting

1.2.2 Threat Analysis

A cross-site scripting incident was detected at Feb 26, 2019, 3:30:56 PM, originating from the source IP of “172.16.11.4”. The destination IP of the event was “172.16.11.37”, indicating that both the attacker and victim are located within the network for TP_IBM_SOC. The offence was logged by SiteProtectorSP3001 in the SOC_Servers. The destination IP is also involved in other offenses which may indicate that the attacker may be carrying out a combination of attacks on the network. Additional investigation is required to elucidate the identity of the user involved in triggering the transfer of data to the destination IP.

1.2.3 Recommendation

This incident is to be escalated to the technical staff in the TP_IBM_SOC simulation lab for further investigation in order to determine the user IDs involved in the cross-site scripting attack, as well as the contents of the data transmitted in the attack. The login credentials and any active sessions of the victim should be reset in case the suspect user has obtained access to that information. Appropriate actions may have to be taken against the suspect user for potentially violating the TP Acceptable User Policy (AUP).

1.2.4 Supporting Data

All Offenses > Offense 19777 (Summary)

Offense 19777 — Summary | Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print

Magnitude		**Status**		**Relevance**	4	**Severity**	9	**Credibility**	2
Description	Cross_Site_Scripting	**Offense Type**	Event Name				
		Event/Flow count	1 events and 0 flows in 1 categories				
Source IP(s)	172.16.11.4	**Start**	Feb 26, 2019, 3:30:56 PM				
Destination IP(s)	172.16.11.37	**Duration**	0s				
Network(s)	TP_IBM_SOC.IBM_SOC_Simulation	**Assigned to**	Unassigned				

Offense Source Summary

Event Name	Cross_Site_Scripting		
High Level Category	Exploit	**Low Level Category**	Cross Site Scripting
Severity	9		
Offenses	7	**Events/Flows**	35

Last 5 Notes — Notes | Add Note

Notes	Username	Creation Date

No results were returned.

Last 5 Search Results — Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows

No results were returned.

Top 5 Source IPs — Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
172.16.11.4		TP_IBM_SOC.IBM_SOC_Simulation	No	Unknown	Unknown NIC	0	21	7	5h 52m 34s	7,231

Top 5 Destination IPs — Destinations

Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
172.16.11.37		TP_IBM_SOC.IBM_SOC_Simulation	No	Yes	Unknown	Unknown NIC	0	9	1	5h 52m 37s	12

Top 5 Log Sources — Log Sources

Name	Description	Group	Events	Offenses	Total Events
SP3001	SiteProtectorSP3001	SOC_Servers	1	281	1,611,007

Top 5 Users — Users

Name	Events/Flows	Offenses	Total Events/Flows

No results were returned.

Top 5 Categories — Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow
Cross Site Scripting		1	1	Feb 26, 2019, 3:30:56 PM	Feb 26, 2019, 3:30:56 PM

Last 10 Events — Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Cross_Site_Scripting		SP3001	Cross Site Scripting	172.16.11.37	56341	Feb 26, 2019, 3:30:56 PM

Last 10 Flows — Flows

Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time

No results were returned.

Top 5 Annotations — Annotations

Annotation	Time	Weight
"Offense Chaining". This offense has 1 destinations (destination IPs), which are the source (attacker)in other offenses	Feb 26, 2019, 3:31:20 PM	7
"Offense Chaining". This source IP currently has 2 other source active on the network.	Feb 26, 2019, 3:31:20 PM	1

Screen capture of Offense 19777: Cross-Site Scripting.

2 Security Intelligence Report

Topic:	**Descriptions/Actions**
Advisory Title:	CVE-2019-1987
Threat Name:	Android Operating System - Remote code execution in privileged process from file
Overview:	Android Framework parsing error when handling PNG file. In the function onSetSampleX of SkSwizzler.cpp which is part of Android Framework, during the parsing of is a possible out of bounds write due to a missing bounds check . This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.
Affected Versions:	• Android-7.0 • Android-7.1.1 • Android-7.1.2 • Android-8.0 • Android-8.1 • Android-9
Affected Assets (Locations):	Devices running Android OS worldwide
Threat Type:	The vulnerability could allow an attacker to send a specially crafted PNG (Portable Network Graphic file) file via messaging apps, email or webpage. If the user opens this file for viewing, remote arbitrary code execution in privileged process can be achieved, resulting in device hijack and compromise.
Threat CVE Links:	• https://nvd.nist.gov/vuln/detail/CVE-2019-1987 • http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1987 • https://source.android.com/security/bulletin/2019-02-01
Threat State:	Certain
Threat Impact:	High
Recommendations:	Android devices be updated with the latest security patch levels 2019-02-01 & 2019-02-05 ASAP, to fix the issues contained in this advisory. As Android is a multiple platform open source OS, an available update for your device may depend on a release from your specific manufacturer.

3 Advancement in SIEM Technologies

3.1 QRadar Advisor with Watson (AI/Machine Learning Solution)

3.1.1 Cognitive Security

QRadar Advisor with Watson extends IBM QRadar Security Intelligence Platform deployment with cognitive security. Now it can go beyond gathering data from users' own systems. Users can supplement it with knowledge created worldwide and with the ability of Watson to use that knowledge to understand, reason, and learn about security topics and threats.

3.1.2 Threat Response

Begin with common sense, insights, and the ability to generalize that comes from human expertise. Add the ability of security analytics to correlate data, identify behavioral patterns and anomalies, and prioritize and manage workflows. Using QRadar Advisor with Watson and IBM Watson for Cyber Security, users can extend their capabilities further with cognitive security's power to analyze unstructured as well as structured data, to understand natural language, and to respond. Users can finally gain the ability to draw upon the huge amount of security information when they previously could not tap the vast majority of security knowledge that is unstructured.

3.1.3 Understanding Threat Behaviour

QRadar detects threats. QRadar Advisor with Watson provides cognitive abilities that can help deal with them. Working together, these technologies can mimic human thought to understand advanced threats, triage threats, and make recommendations about dealing with potential or actual attacks. For example, a malware-borne strike attempting to access and exfiltrate intellectual property can be caught by QRadar. QRadar Advisor with Watson then makes it possible to analyze structured and unstructured information to identify the threat, understand how that threat behaves, uncover indicators that occur in the typical attack chain, and analyze how the attack may have progressed.

3.1.4 Intelligence

Some potential threats are easy to resolve. A weekend attempt to access the database may simply be an employee working from home. QRadar can detect unusual behavior, then an analyst can decide whether it's dangerous. For sophisticated attacks, the cognitive techniques of QRadar Advisor with Watson can help to ingest and correlate vast amounts of structured and unstructured security data available to uncover new threat patterns, triage threats and make recommendations. QRadar Advisor with Watson provides a solution that not only ingests data, but also reasons and derives its own knowledge from it, discovering linkages that may otherwise go unnoticed and presenting information most relevant to the investigation.

3.1.5 Accuracy

A security system is only as trustworthy as it is accurate, both at consistently detecting actual threats, and at rejecting false positives. Cybercriminals rely on slipping through the same channels as legitimate users and applications, because they know you can't examine every packet in advance. QRadar Advisor with Watson gives the benefit of highly evolved detection and verification techniques. X-Force security researchers analyze hundreds of millions of data points to address both sides of the detection coin.

3.1.6 Speed

Even the most accurate intelligence is worthless if it's delivered too late. Dedicated, always-on monitoring systems can alert security personnel in near real time. QRadar Advisor with Watson assists with threat analysis. It enables user to navigate the knowledge Watson has that pertains to a specific security incident, evaluate the evidence, and provide analysts with insights in minutes rather than the hours or days conventional approaches require.