Bhutan Computer Incident Response Team

Bi-Annual Report

June-December 2017

Phone: +975-02-338606
Email: info@btcirt.bt or cirt@btcirt.bt

Table of Content

1. EXECUTIVE SUMMARY

The report captures all essential activities undertaken by BtCIRT from July to December 2017. The overall mission of BtCIRT is to enhance cyber security in Bhutan by enabling cybersecurity information coordination and by establishing computer security incident handling capabilities within the country. Inline with its mission, BtCIRT has conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted security awareness program targeting end users, developed security baseline and conducted organisational security assessment of some of the organisations.

2. Activities and operations

2.1. Security Advisory and Alerts

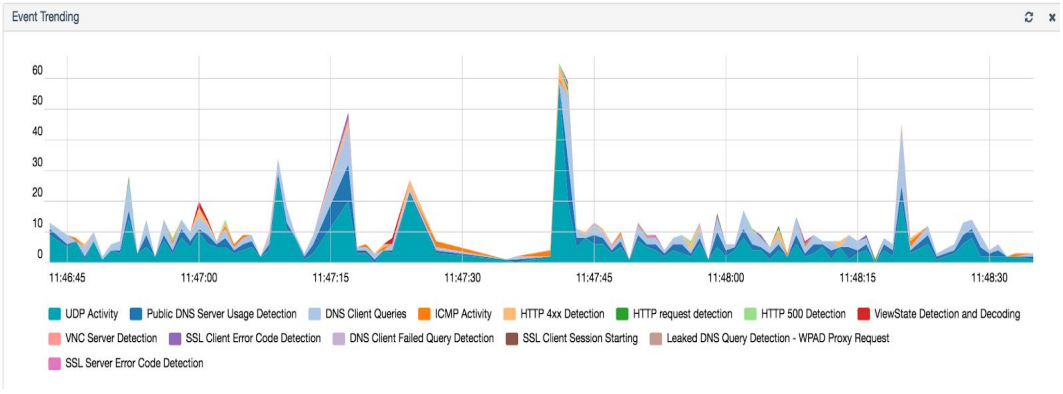
BtCIRT has published 42 security alerts including vulnerability update and latest threats on website and facebook. Constituents can also view Latest CyberSecurity news and vulnerabilities right from BtCIRT website.
BtCIRT has also published 5 security advisories based on common threats and vulnerabilities noted through threat and vulnerability monitoring. Email advisories are also sent to government and critical sector ICT official as and when there are critical attacks. 2 end user advisories were sent to govt ICT heads for dissemination to all the officials under their organisation.

2.2. Incident Management and Response

2.2.1. Services to GDC (Government Data Centre)

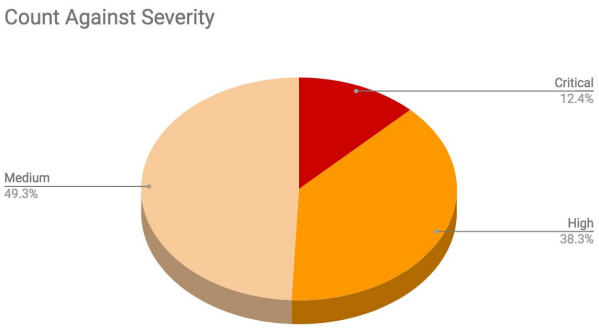
BtCIRT actively monitors Government Data centre for threats and vulnerabilities in both systems and network informs GDC team if any issues detected

2.2.1.1. Monitor system activity for unusual pattern

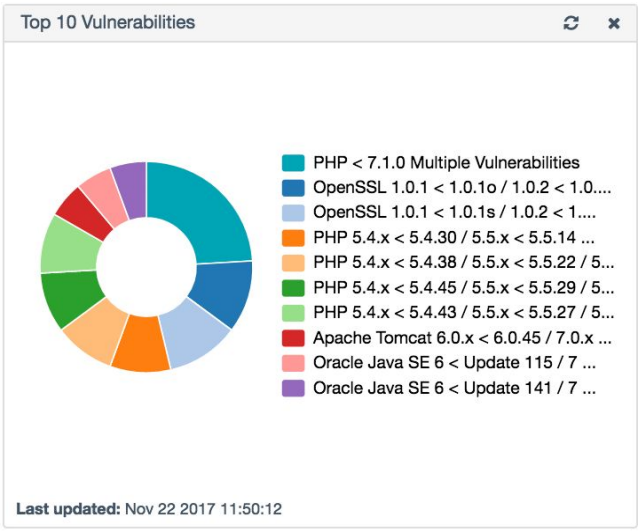


2.2.1.2. Monitor for Vulnerability:

Vulnerabilities are categorized into “Critical”, “Medium”, “High” and “Low” based on how adverse the impact would be if the vulnerability is exploited. Vulnerability of either Critical, high or medium severity were detected in 42 vulnerable systems.



2.2.1.2.1. Top Ten vulnerabilities:



2.2.1.2.2. Top Ten critical Vulnerabilities

Actions | Filter Vulnerabilities

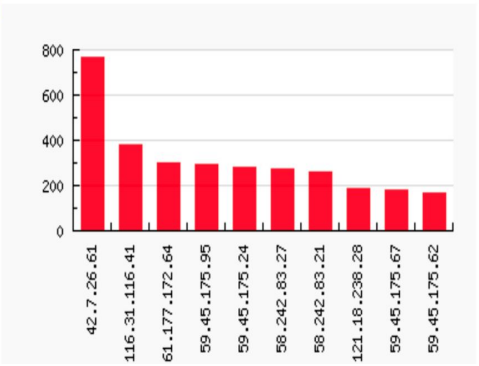
☐	CRITICAL	PHP < 7.1.0 Multiple Vulnerabilities	Web Servers	13
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1o / 1.0.2 < 1.0.2c ASN.1 Encoder Negative Zero Value Handling RCE	Web Servers	6
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1s / 1.0.2 < 1.0.2g RCE	Web Servers	6
☐	CRITICAL	PHP 5.4.x < 5.4.30 / 5.5.x < 5.5.14 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.38 / 5.5.x < 5.5.22 / 5.6.x < 5.6.6 Multiple Vulnerabilities (GHOST)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.43 / 5.5.x < 5.5.27 / 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.45 / 5.5.x < 5.5.29 / 5.6.x < 5.6.13 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	Apache Tomcat 6.0.x < 6.0.45 / 7.0.x < 7.0.68 / 8.0.x < 8.0.32 Multiple Vulnerabilities	Web Servers	3
☐	CRITICAL	Oracle Java SE 6 < Update 115 / 7 < Update 101 / 8 < Update 92 Multiple Vulnerabilities	Web Clients	3
☐	CRITICAL	Oracle Java SE 6 < Update 141 / 7 < Update 131 / 8 < Update 121 Multiple Vulnerabilities	Web Clients	3

2.2.1.3. Perform Authenticated scan for systems before hosting at GDC and on request basis:
7 Systems were assessed for Vulnerabilities and detailed report provided to system owner

2.2.1.4. Monitor for threats and attacks:
GDC has faced two major cyber attack within last 6 months. With threat monitoring we were able to identify compromised system and resolve the issue. We were also able find out most attacked services and apply necessary technical measure to mitigate the same. It was noticed that ssh and RDP services were used to initiate so much of traffic affecting the availability of systems hosted there.

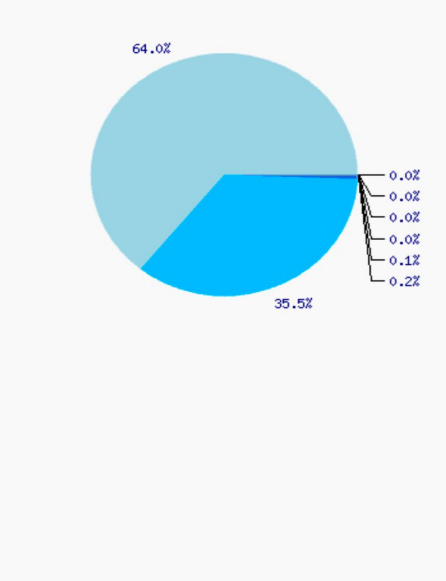
Alarms Report - Top 10 Attacker Host from: 2017-08-07 to: 2017-09-06

Host	Occurrences
42.7.26.61	770
116.31.116.41	380
61.177.172.64	299
59.45.175.95	293
59.45.175.24	277
58.242.83.27	274
58.242.83.21	259
121.18.238.28	186
59.45.175.67	183
59.45.175.62	168



Alarms Report - Top 15 Alarms from: 2017-08-07 to: 2017-09-06

Alarm	Occurrences
Delivery & Attack — Bruteforce Authentication — SSH	4.103
Delivery & Attack — Bruteforce Authentication — Linux/Unix	2.278
Reconnaissance & Probing — Service discovery — Microsoft Remote Desktop	16
Delivery & Attack — Bruteforce Authentication — Microsoft Remote Desktop	6
Reconnaissance & Probing — Service discovery — VNC	2
Reconnaissance & Probing — Service discovery — SSH	1
Delivery & Attack — WebServer Attack - SQL Injection — Attack Pattern Detection	1
Exploitation & Installation — WebServer Attack — XSS	1



2.2.1.5. Vulnerability Management Process developed and provided to GDC

2.2.2. Services to GovNet and other gov agencies:

2.2.2.1. We provide services to other constituents on request basis and when we are reported by external agencies.

2.2.2.2. We identified vulnerabilities or malware infection in 25 systems and reported to systems owner for necessary action.

2.2.2.3. Security Assessment was carried out for Kuensel Corporation Limited and details report of vulnerabilities and mitigation measure was provided.

2.2.2.4. Scam and phishing

2.2.2.4.1. One of our constituent reported that their finance head received an email requesting for wire transfer with the sender impersonating as their ex-CEO. On analysis it was found that the email originated from Africa and used an email server in US (earthlink.net). The email ms092@earthlink.net could be a compromised email.

2.2.2.4.2. PhishLabs reported that they have identified a form receiver file which was hosted on IP belonging to Bhutan and attempting to defraud the customers of Wells Fargo Personal Banking. This form receiver file was detected as part of a phishing site that is copying a legitimate Wells Fargo Personal Banking site, and used to route stolen credentials to the attacker as the victim inputs them into the fraudulent site. BtCIRT with support from ISP suspended the site.

2.2.2.4.3. One of our constituents also reported of receiving scam call, BtCIRT requested ISPs support and advised the client not to Receive/Call Back or provide any information to unknown numbers.

2.2.3. A test lab has been setup where web, mail and DNS test servers are hosted for testing any incident related to these services. A ssh honeypot sensor has also been implemented to study the behaviour of attackers, which shall be extended with other sensors.

3. Events Organised

3.1. Workshops:

3.1.1. Information and network security Workshop

was conducted With financial support from EU(European Union) and TEIN*CC @TEIN (Trans-Eurasia Information Network* Corporation Center) through the Asi@Connect Project and Technical support from APNIC from 9th- 13th October, 2017. The workshop covered topics on Network and Security threats and breaches, Policies and Countermeasures with practical sessions on identifying and defending threats and vulnerabilities. 50 ICT officers from various sectors including Banks, Power Corporation, Royal Bhutan Police, RUB Colleges, Dzongkhags and Ministries attended the session.

3.2. Events attended:

3.2.1. 8th Cyber Security Forum organized APT.

4. International Collaboration

4.1. Member of APCERT(Asia Pacific Computer Emergency Response Team) and FIRST(Forum of Incident Response and Security Teams)

5. Future Plans:

5.1. Awareness programs in 13 dzongkhags
5.2. Security Incident Mock Drill
5.3. IMSP review
5.4. FINCERT consultative meeting
5.5. Security assessment for 2 ministries
5.6. Workshop on secure Coding

6. Contact:

Address:

Bhutan Computer Incident Response Team(BtCIRT)
Infrastructure Division
Department of Information Technology and Telecom (DITT)
Ministry of Information and Communications
Thori Lam, Chubachu, Thimphu
Bhutan, Post Box: 482

Phone: +975-02-338606
Email: info@btcirt.bt (for general questions)
Email: cirt@btcirt.bt (for reporting an incident)
In case of sensitive information please use BtCIRT PGP key to encrypt your content.

Working hours: 9:00-17:00, Monday to Friday (BTT/Bhutan Time, UTC+6, no DST)
You will receive email notifications for any new articles we post if you subscribe through our website.
Get notified as you socialize on facebook by following our page "Bhutan Computer Incident Response Team"