**What are the targets?**

Targets

Node file in distribution systems

System Files

Kernel Memory

Socket buffer

Kernel stack memory

Memory

Database

Cryptographic objects

Special objects

Android Activity

TMP File

Lock File

Configuration File

Html/Web script

Executable Code

Files

Assets

Code Segment

Application Files

System-Level

Application-Level

Operating system commands

Type casting

Serialization/deserialization

Deserializing polymorphic class

Gadget classes

Memory manipulation

Loops counting buffer size

Uninitialized memory

**Where are the entry points? (code-level)**

Entry points

Inter-procedural communication

Service request

Rest APIs

HTTP post requests

HTTP get requests

Web requests

DLL Files

Electronic Datasheet (EDS) files

Requests

Command line arguments

Files

Device related arguments

IPv6 Packet

Network Sockets

Packets

Account information file

(ex. etc/passwd)

System files

Device-level

Network-Level

System-level

Application-level

**Where are the entry points? (design-level)**

Entry points components

Plugin administration

Text editors

Chat features

File system handling

System Interaction

Configuration components

Update

Installer

Installer components

User Interfaces

User Console

Web Console

File upload

Console

Port management

Network Management

**How does the exploit happen?**

How

Type

Do not checking/handle input

Dynamic SQL query creation

Mismatched type casting

CSS filters

Encryption libraries

Send multiple packets in a short time

request

Send multiple request in a short time

packets

Size

File

HTTP instead of HTTPS

Protocols

Symlinks

Dangerous programming techniques/errors

Uses of unsafe technologies

Uses of third-party

libraries

Unauthenticated access to accounts or services

Improper permission for running scripts

Improper permission for accessing file

Access/permissions