What?

1. Software configuration parts:
2. Special Objects or Classes: Cryptographic objects, Gadget Classes
3. Sensitive/private information: Credentials, userdata, metadata
4. Operating system commands (system calls)
5. Software application files: lock files, tmp files,
6. System files: node catalog in distributed systems
7. HTML/Webscripts
8. Memory allocation/deallocation/tampering/access: socket buffer, kernel memory, kernel stack memory, loops counting buffer size, uninitialized memory, check boundary??
9. Web shell
10. Marshalling/unmarshalling data objects to/from json: deserializing class, deserializing polymorphic class
11. Android activity
12. Type casting parts
13. Part of source code to be run
14. database

Architectural: add admin user

Port interface management part of the operating systems

Where?)

1. System files: account information file (etc/passwd), dll files, eds files
2. Command line arguments
3. Web requests: http post request, http get request, files in post requests
4. Packets: IPv6 packets
5. Network sockets
6. REST APIs
7. Device related arguments
8. Service requests: such as inter procedural communication

Design-level (system sub-modules):

1. Application Configuration
2. File system handling
3. Installer components
4. Update component
5. Editor
6. Chat
7. User Console
8. Web console
9. Plugin administration
10. Local access
11. Port management interface
12. File upload

How

1. Using third party library: encryption package
2. Improper permission: for accessing files, running scripts
3. Run executables based on accessible configuration files
4. Mismatched type casting
5. Dynamic SQL query creation
6. Do not checking input file: type, size
7. Using dangerous technology: CSS filters, symlinks
8. Using incorrect (unsafe) technology: http instead of https
9. Unauthenticated access to account or services
10. Sending multiple requests or packets together in short time

Input data:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Tiff file | CVE-2020-6067 | Out-of-bounds Write |
|  | XML | CVE-2020-6238 | CWE-20Improper Input Validation |
|  | BLOB  A binary large object (blob) is concentrated binary data that’s compressed into an individual file inside a database. The large size of the file means they need special storage treatment. Blobs are binary, which means they are usually images, audio or other media. | CVE-2020-7248 | Out-of-bounds Write |
|  | YAML  It’s basically a human-readable structured data format. It is less complex and ungainly than XML or JSON, but provides similar capabilities. It essentially allows you to provide powerful configuration settings, without having to learn a more complex code type like CSS, JavaScript, and PHP. | CVE-2020-1947 | CWE-502-Deserialization of Untrusted Data |
|  | Android Parcel  Android Parcel would be that of a message container for lightweight, high-performance Inter-process communication (IPC). . | CVE-2020-0017 | CWE-200- Exposure of Sensitive Information to an Unauthorized Actor |
|  | JSON | CVE-2019-10749  CVE-2019-10748 | CWE-89- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
|  | CVE-2018-7489 | CWE-184- Incomplete List of Disallowed Inputs |
|  |  | CVE-2018-18836 | CWE-74- Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |
|  | CVE-2017-18349 | CWE20-Improper Input Validation |
|  | CVE-2017-17485 | CWE-502- Deserialization of Untrusted Data |
|  | CVE-2014-5017 | CWE-89- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
|  |  | CVE-2014-3994 | CWE-79- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
|  | IPv4 packet | CVE-2020-1638 | CWE20-Improper Input Validation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | installation options |  |  |