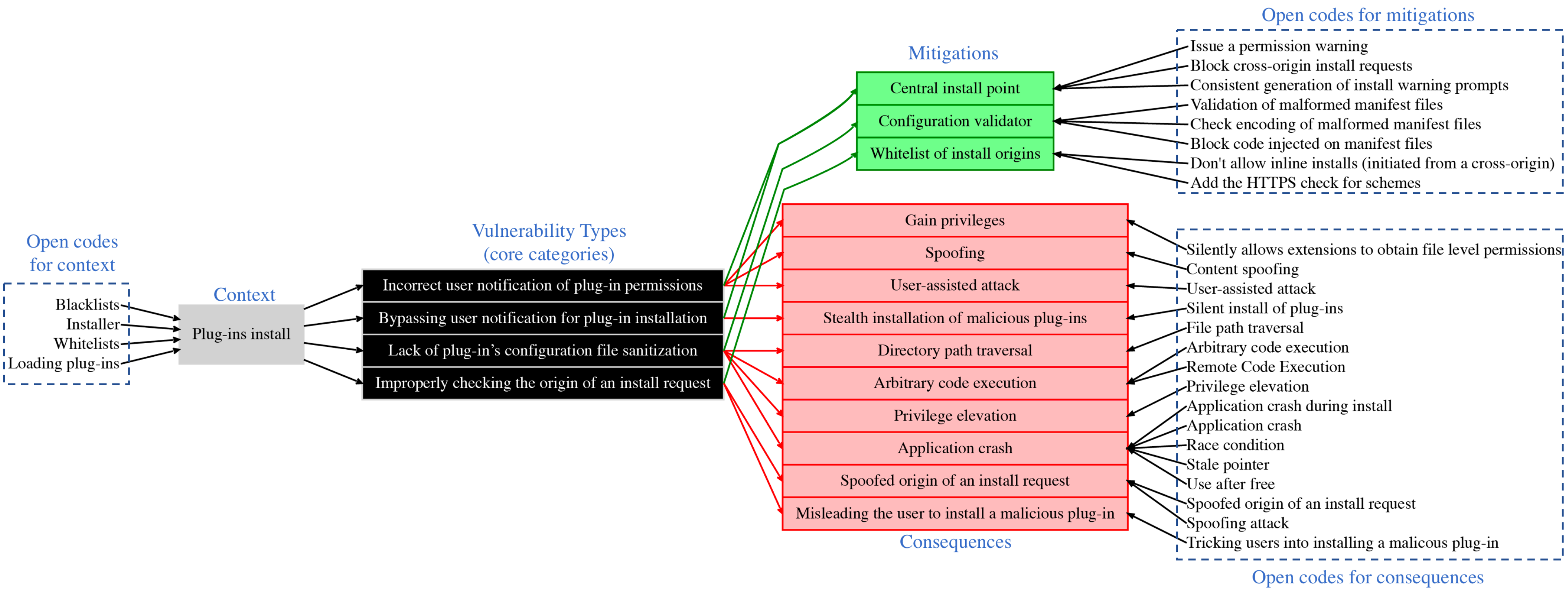
Theoretical coding is the process of interconnecting concepts that integrate our theory. Therefore, **a theoretical code is the relationship between two or more concepts**. A concept is either a core category or a substantive code.

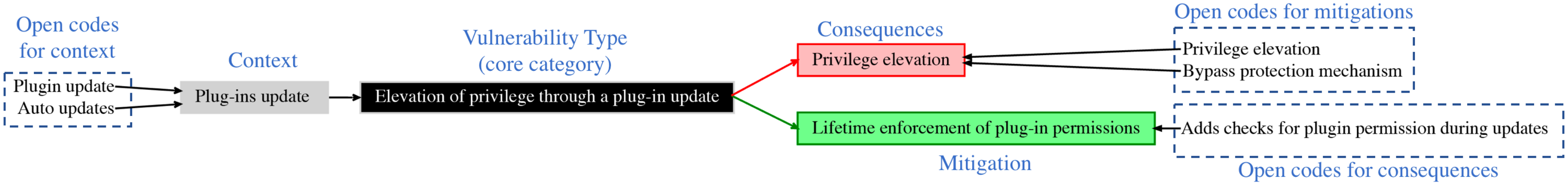
We follow a theoretical coding in which, for each core category (vulnerability type), we identify its context, mitigations, consequences. Therefore, to derive our theoretical codes, we first look back at the output of our open coding process and memos and then start interconnecting these concepts to the core categories by verifying whether the concept corresponds to the *context*, a *consequence* or a *mitigation* of the vulnerability (See Table I). Through an iterative process of interconnecting these concepts to the core categories, we are able to derive our theory. We demonstrate our theoretical coding process of interconnecting concepts (starting out from our disconnected open concepts to fully integrated concepts through a diagram (which depicts these relationships).

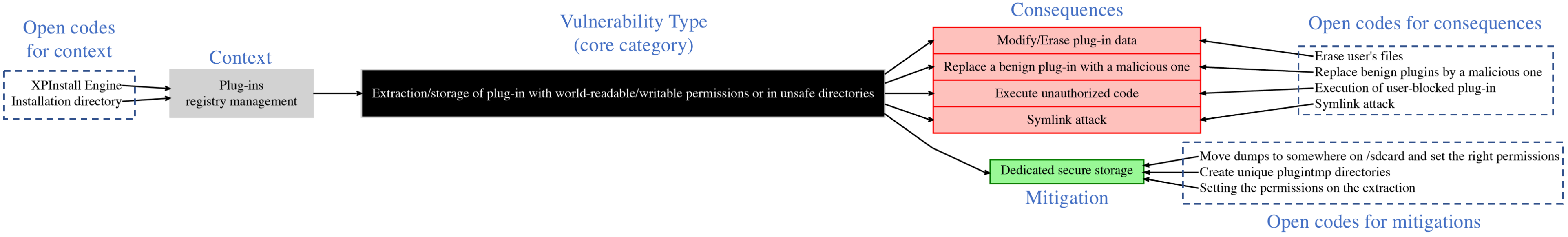
Table I: Mapping of open codes to our coding paradigm (context, consequence, mitigation)

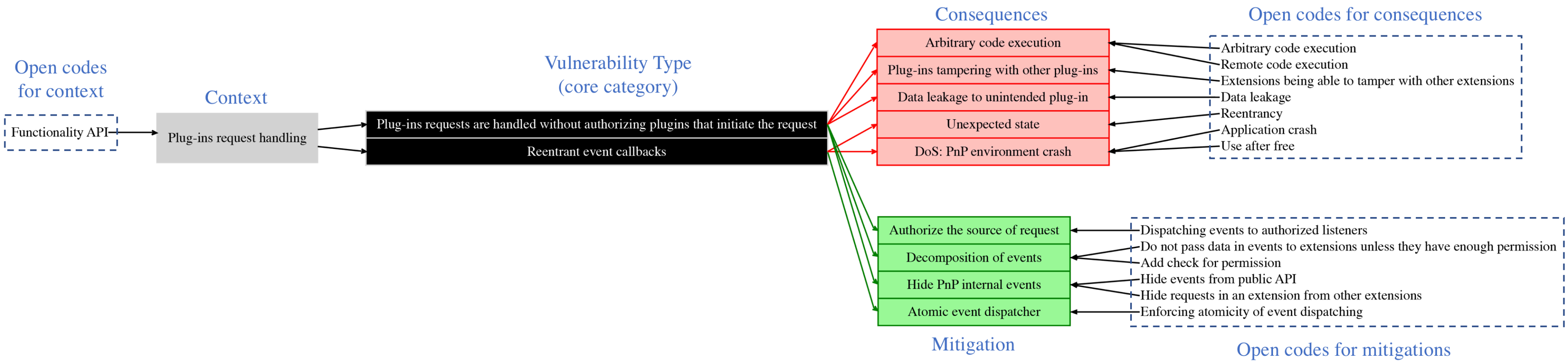
Mapped To	Open Code	Associated CVEs
Context	Blacklists	CVE-2011-3049
Context	Installer	CVE-2004-0762,CVE-2004-0906,CVE-2005-0590,CVE-2006-2784,CVE-2010-3417,CVE-2010-4491,CVE-2011-1815,CVE-2011-2370,CVE-2011-2785,CVE-2011-2789,CVE-2011-3001,CVE-2013-0798,CVE-2013-0831,CVE-2013-0924,CVE-2015-0812,CVE-2016-1640,CVE-2016-1948
Context	Loading plug-ins	CVE-2011-3047
Context	Plugin update	CVE-2013-2868
Context	Uninstaller	CVE-2011-0470
Context	IPC Service	CVE-2010-1229,CVE-2011-3080,CVE-2013-2866
Context	JS Objects Isolation	CVE-2010-0170,CVE-2010-2110,CVE-2011-3107,CVE-2012-1956,CVE-2012-3994,CVE-2012-4194,CVE-2015-4495,CVE-2016-1622
Context	Plug-in interaction	CVE-2010-1198
Context	Object deallocation	CVE-2009-1837,CVE-2010-0177,CVE-2011-1450,CVE-2011-1813,CVE-2011-2789,CVE-2011-2853,CVE-2012-3960,CVE-2012-5125,CVE-2012-5126,CVE-2014-7935,CVE-2015-2706
Context	Object wrappers	CVE-2008-2803,CVE-2009-2665,CVE-2011-3004,CVE-2016-1966
Context	Reentrancy	CVE-2013-2912,CVE-2015-6772,CVE-2016-1635
Consequence	Sandbox escape	CVE-2010-1229,CVE-2010-4491,CVE-2011-3080,CVE-2014-1728,CVE-2014-8643,CVE-2015-1226
Consequence	Remote Code Execution	CVE-2008-6811,CVE-2010-1229,CVE-2011-3981,CVE-2011-4342,CVE-2012-0934
Consequence	Same-Origin Policy Bypass	CVE-2008-2806,CVE-2010-0170,CVE-2011-3080,CVE-2011-3956,CVE-2013-0747,CVE-2015-1302,CVE-2015-4495,CVE-2015-6772,CVE-2016-1622,CVE-2016-1949
Consequence	Alter Execution Logic	CVE-2016-1622
Mitigation	Block cross-origin install requests	CVE-2015-4498
Consequence	Application crash	CVE-2008-4062,CVE-2008-5013,CVE-2009-2852,CVE-2010-0161,CVE-2010-0173,CVE-2010-1198,CVE-2010-4491,CVE-2011-0470,CVE-2011-0475,CVE-2011-0779,CVE-2011-1124,CVE-2011-1450,CVE-2011-1813,CVE-2011-2789,CVE-2011-2853,CVE-2011-3107,CVE-2012-2877,CVE-2012-2878,CVE-2012-2880,CVE-2012-2881,CVE-2012-5111,CVE-2012-5125,CVE-2013-0801,CVE-2013-0837,CVE-2013-0919,CVE-2013-2841,CVE-2013-2912,CVE-2014-1519,CVE-2015-2706,CVE-2015-2709,CVE-2015-7196,CVE-2016-1635,CVE-2016-1650,CVE-2016-1966
Consequence	Application crash during install	CVE-2010-4575
Mitigation	Check object is not null	CVE-2010-4575,CVE-2011-1450,CVE-2011-3107,CVE-2012-2877,CVE-2012-2878,CVE-2014-1519,CVE-2015-2709
Consequence	Execution of user-blocked plug-in	CVE-2010-2108,CVE-2013-0910
Mitigation	Passing user-defined blocked plugins info to app host	CVE-2010-2108
Mitigation	Consistent generation of install warning prompts	CVE-2011-3055
Consequence	Privilege elevation	CVE-2005-0232,CVE-2007-3844,CVE-2009-2665,CVE-2010-1585,CVE-2011-1819,CVE-2011-3004,CVE-2012-2816,CVE-2013-2868,CVE-2013-3491,CVE-2014-3170,CVE-2014-8643,CVE-2015-7223
Consequence	Arbitrary code execution	CVE-2005-0752,CVE-2007-5045,CVE-2007-5800,CVE-2008-2806,CVE-2008-5013,CVE-2008-5695,CVE-2009-1310,CVE-2009-1837,CVE-2009-2396,CVE-2009-2665,CVE-2010-0177,CVE-2011-0012,CVE-2011-0059,CVE-2011-1179,CVE-2011-1815,CVE-2011-2785,CVE-2011-3001,CVE-2011-3961,CVE-2011-5107,CVE-2012-0446,CVE-2012-3960,CVE-2012-4263,CVE-2012-4264,CVE-2013-3529,CVE-2013-4954,CVE-2013-7279,CVE-2014-1519,CVE-2015-7196,CVE-2017-12796
Consequence	Steal data	CVE-2005-0752,CVE-2011-5107,CVE-2011-5264,CVE-2012-1785,CVE-2012-4268,CVE-2013-0925,CVE-2013-3529,CVE-2015-7223,CVE-2016-1949

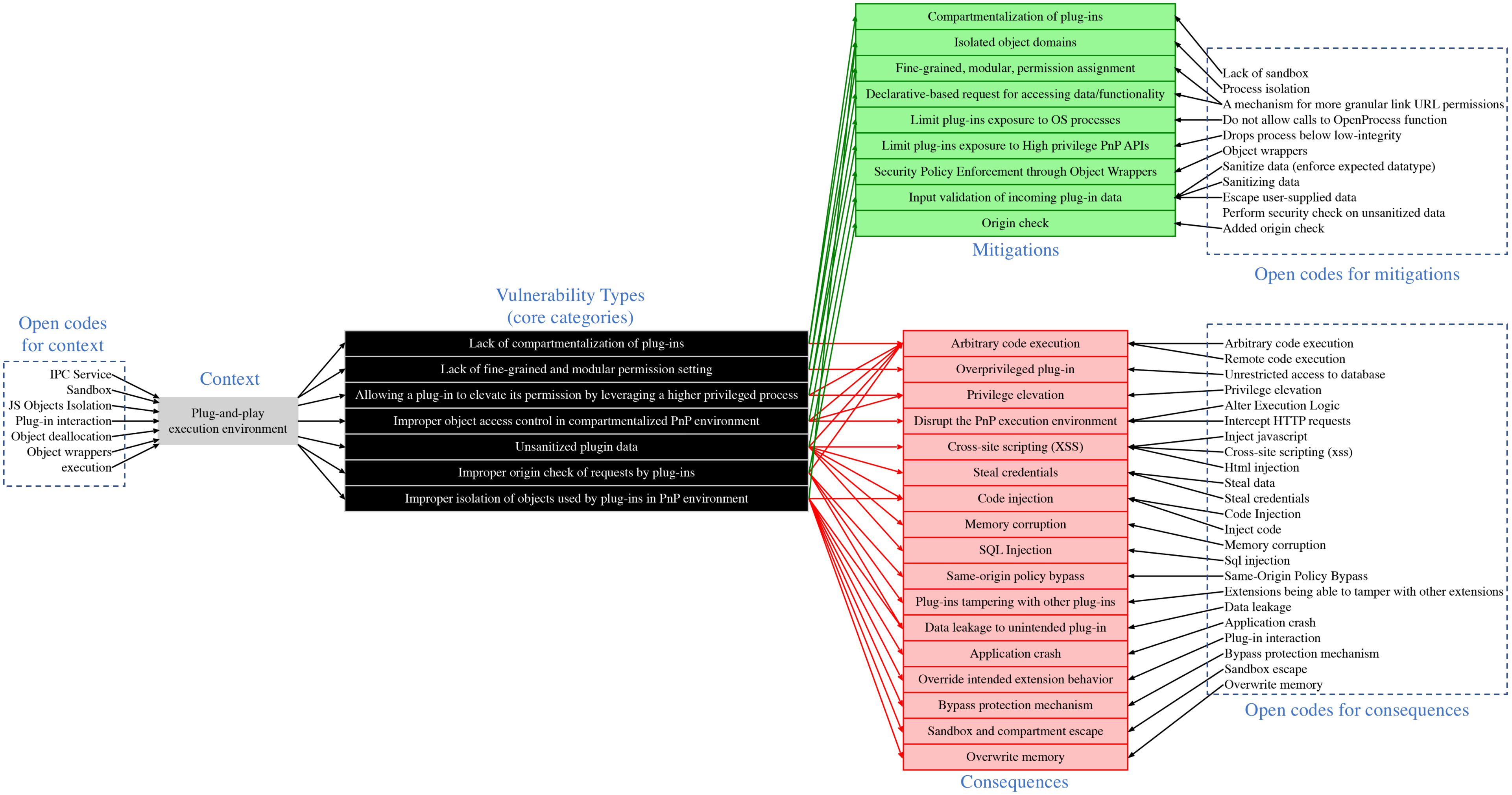
Mitigation	Perform security check on unsanitized data	CVE-2005-0752,CVE-2010-1585,CVE-2011-5191,CVE-2011-5225,CVE-2011-5264,CVE-2012-4272,CVE-2012-4273,CVE-2013-0896,CVE-2017-12796
Consequence	Memory corruption	CVE-2011-3047,CVE-2013-0896,CVE-2014-1519
Consequence	Steal credentials	CVE-2011-5107,CVE-2013-3262,CVE-2013-3529,CVE-2013-4954,CVE-2013-5098,CVE-2013-7279
Mitigation	Escape user-supplied data	CVE-2008-0491,CVE-2008-1982,CVE-2011-4562,CVE-2011-5192,CVE-2012-2920,CVE-2012-4271,CVE-2012-5327,CVE-2013-3526,CVE-2013-4954
Mitigation	Sanitizing data	CVE-2013-5098
Mitigation	Sanitize data (enforce expected datatype)	CVE-2008-1982,CVE-2008-4625,CVE-2009-2122,CVE-2009-2383,CVE-2011-5106,CVE-2012-1068,CVE-2012-2759,CVE-2012-4263,CVE-2012-6527
Consequence	File path traversal	CVE-2006-5705,CVE-2008-5752,CVE-2008-6811,CVE-2009-4672,CVE-2012-0934,CVE-2013-5963
Consequence	User-assisted attack	CVE-2004-0762,CVE-2005-0232,CVE-2006-2784,CVE-2011-3001,CVE-2012-6527,CVE-2015-1298
Consequence	Man-in-the-middle attack	CVE-2015-0812,CVE-2016-1948
Consequence	Intercept HTTP requests	CVE-2016-1949
Consequence	Race condition	CVE-2009-1837,CVE-2011-0470,CVE-2012-2880,CVE-2015-2706,CVE-2016-1650
Consequence	Use after free	CVE-2011-1124,CVE-2012-2878,CVE-2012-2881,CVE-2012-3960,CVE-2012-5126,CVE-2014-7935,CVE-2015-2706,CVE-2015-6772
Consequence	Stale pointer	CVE-2011-1813
Mitigation	Notify deallocation events	CVE-2011-1813
Mitigation	Process Isolation	CVE-2012-2877
Mitigation	Changing the order of deallocation of objects	CVE-2012-2877
Consequence	Data leakage	CVE-2008-2807,CVE-2009-2334,CVE-2010-3250,CVE-2010-3417,CVE-2011-0076,CVE-2011-1435,CVE-2011-1819,CVE-2011-2853,CVE-2011-3080,CVE-2012-3973,CVE-2012-3975,CVE-2013-0831,CVE-2013-2876,CVE-2013-5598,CVE-2015-1302,CVE-2015-4495
Consequence	Overwrite memory	CVE-2006-6499
Consequence	Bypass protection mechanism	CVE-2005-0232,CVE-2011-0076,CVE-2011-1123,CVE-2011-1435,CVE-2011-2785,CVE-2011-3001,CVE-2013-0731,CVE-2013-2868,CVE-2013-2876,CVE-2014-3170,CVE-2014-3172,CVE-2015-1226,CVE-2015-6779,CVE-2015-7187,CVE-2016-1638,CVE-2016-1640
Consequence	Silently allows extensions to obtain file level permissions	CVE-2013-0924
Mitigation	Enforcing atomicity of event dispatching	CVE-2016-1635
Consequence	Code Injection	CVE-2010-0179,CVE-2010-4747,CVE-2010-5295,CVE-2011-1815,CVE-2011-1819,CVE-2011-2785,CVE-2011-4618,CVE-2011-4646,CVE-2017-12796,CVE-2017-15714
Consequence	Replace benign plugins by a malicious one	CVE-2004-0906,CVE-2013-0798
Consequence	Bypassing restrictions on debugging remotely	CVE-2012-3973
Consequence	Tricking user into installing a malicous plug-in	CVE-2005-0590,CVE-2016-1640
Consequence	Erase user's files	CVE-2005-0578
Consequence	Symlink attack	CVE-2005-0578
Consequence	Extensions being able to tamper with other extensions	CVE-2014-3172,CVE-2015-1297
Consequence	Allowing extensions to debug tabs	CVE-2015-1226
Consequence	Trigger access to an arbitrary URL	CVE-2012-3975,CVE-2015-1298,CVE-2015-6779
Mitigation	Added origin check	CVE-2010-0179,CVE-2010-3250,CVE-2014-1728
Consequence	Read user's files	CVE-2011-1435
Consequence	Prevent blacklists from being updated	CVE-2011-3049
Mitigation	Monitoring crashes on plug-ins	CVE-2012-5111
Consequence	Overwrite files	CVE-2013-2741
Consequence	Content spoofing	CVE-2013-2204
Consequence	inject code	CVE-2011-4342


Open codes for context
Blacklists
Installer
Whitelists
Loading plug-ins
Context
Plug-ins install
Vulnerability Types (core categories)
Incorrect user notification of plug-in permissions
Bypassing user notification for plug-in installation
Lack of plug-in’s configuration file sanitization
Improperly checking the origin of an install request
Mitigations
Central install point
Configuration validator
Whitelist of install origins
Open codes for mitigations
Issue a permission warning
Block cross-origin install requests
Consistent generation of install warning prompts
Validation of malformed manifest files
Check encoding of malformed manifest files
Block code injected on manifest files
Don't allow inline installs (initiated from a cross-origin)
Add the HTTPS check for schemes
Gain privileges
Spoofing
User-assisted attack
Stealth installation of malicious plug-ins
Directory path traversal
Arbitrary code execution
Privilege elevation
Application crash
Spoofed origin of an install request
Misleading the user to install a malicious plug-in
Consequences
Silently allows extensions to obtain file level permissions
Content spoofing
User-assisted attack
Silent install of plug-ins
File path traversal
Arbitrary code execution
Remote Code Execution
Privilege elevation
Application crash during install
Application crash
Race condition
Stale pointer
Use after free
Spoofed origin of an install request
Spoofing attack
Tricking users into installing a malicous plug-in
Open codes for consequences


Open codes for context
Plugin update
Auto updates
Context
Plug-ins update
Vulnerability Type (core category)
Elevation of privilege through a plug-in update
Consequences
Privilege elevation
Open codes for mitigations
Privilege elevation
Bypass protection mechanism
Lifetime enforcement of plug-in permissions
Mitigation
Adds checks for plugin permission during updates
Open codes for consequences


Open codes for context
XPInstall Engine
Installation directory
Context
Plug-ins registry management
Vulnerability Type (core category)
Extraction/storage of plug-in with world-readable/writable permissions or in unsafe directories
Consequences
Modify/Erase plug-in data
Replace a benign plug-in with a malicious one
Execute unauthorized code
Symlink attack
Open codes for consequences
Erase user's files
Replace benign plugins by a malicious one
Execution of user-blocked plug-in
Symlink attack
Dedicated secure storage
Mitigation
Move dumps to somewhere on /sdcard and set the right permissions
Create unique plugintmp directories
Setting the permissions on the extraction
Open codes for mitigations


Open codes
for context
Functionality API
Context
Plug-ins request handling
Vulnerability Type
(core category)
Plug-ins requests are handled without authorizing plugins that initiate the request
Reentrant event callbacks
Consequences
Arbitrary code execution
Plug-ins tampering with other plug-ins
Data leakage to unintended plug-in
Unexpected state
DoS: PnP environment crash
Open codes for consequences
Arbitrary code execution
Remote code execution
Extensions being able to tamper with other extensions
Data leakage
Reentrancy
Application crash
Use after free
Authorize the source of request
Decomposition of events
Hide PnP internal events
Atomic event dispatcher
Mitigation
Dispatching events to authorized listeners
Do not pass data in events to extensions unless they have enough permission
Add check for permission
Hide events from public API
Hide requests in an extension from other extensions
Enforcing atomicity of event dispatching
Open codes for mitigations


Compartmentalization of plug-ins
Isolated object domains
Fine-grained, modular, permission assignment
Declarative-based request for accessing data/functionality
Limit plug-ins exposure to OS processes
Limit plug-ins exposure to High privilege PnP APIs
Security Policy Enforcement through Object Wrappers
Input validation of incoming plug-in data
Origin check
Mitigations
Lack of sandbox
Process isolation
A mechanism for more granular link URL permissions
Do not allow calls to OpenProcess function
Drops process below low-integrity
Object wrappers
Sanitize data (enforce expected datatype)
Sanitizing data
Escape user-supplied data
Perform security check on unsanitized data
Added origin check
Open codes for mitigations
Open codes
for context
IPC Service
Sandbox
JS Objects Isolation
Plug-in interaction
Object deallocation
Object wrappers
execution
Context
Plug-and-play
execution environment
Vulnerability Types
(core categories)
Lack of compartmentalization of plug-ins
Lack of fine-grained and modular permission setting
Allowing a plug-in to elevate its permission by leveraging a higher privileged process
Improper object access control in compartmentalized PnP environment
Unsanitized plugin data
Improper origin check of requests by plug-ins
Improper isolation of objects used by plug-ins in PnP environment
Arbitrary code execution
Overprivileged plug-in
Privilege elevation
Disrupt the PnP execution environment
Cross-site scripting (XSS)
Steal credentials
Code injection
Memory corruption
SQL Injection
Same-origin policy bypass
Plug-ins tampering with other plug-ins
Data leakage to unintended plug-in
Application crash
Override intended extension behavior
Bypass protection mechanism
Sandbox and compartment escape
Overwrite memory
Consequences
Arbitrary code execution
Remote code execution
Unrestricted access to database
Privilege elevation
Alter Execution Logic
Intercept HTTP requests
Inject javascript
Cross-site scripting (xss)
Html injection
Steal data
Steal credentials
Code Injection
Inject code
Memory corruption
Sql injection
Same-Origin Policy Bypass
Extensions being able to tamper with other extensions
Data leakage
Application crash
Plug-in interaction
Bypass protection mechanism
Sandbox escape
Overwrite memory
Open codes for consequences