|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Fields | Valid Data Values | | | |
| **DocumentVersion** | Version number to keep track of when new fields are added / changed | | | |
| **Vendor** | Vendor Name | | | |
| **Platform** | z/Architecture, iSeries, etc | | | |
| **OperatingSystem** | z/OS, zLinux, zVM, etc | | | |
| **InitialPublicationDate** | Date the CVE or Vulnerability was first published in ISO 8601 format (yyyy-mm-dd). | | | |
| **UniqueIssueIdentifierType** | The type of externally (customer) searchable/trackable reference identifier (i.e. APAR, Security Notice, Case, Custom).  Describes ***UniqueIssueIdentifier.*** | | | |
| **UniqueIssueIdentifier** | The externally (customer) searchable/trackable reference identifier. (i.e. APAR #, Security Notice #, Case # etc..) | | | |
| **ImpactedComponents** | Array of components/products affected by the ***UniqueIssueIdentifier.***  Unique ***ComponentName***, ***ComponentID, ComponentVersions*** combinations have their own objects. When a *Resolution* applies to multiple ***ComponentVersions****,* both versions can be contained within the ***ComponentVersions***array*.* | | | |
| **ComponentType** | | Hardware, Software, Firmware, etc | |
| **ComponentName** | | This is the product or z/OS component name. | |
| **ComponentID** | | For SMP/E products, this is the FMID Identifier (if applicable)  For Non-SMP/E products, “N/A” | |
| **ComponentVersions** | | The component version(s) affected by this vulnerability | |
| **ParentProductName** | | Name of the parent product if the impacted component is a subcomponent of another product. If N/A, this field is contains “N/A”. | |
| **ParentProductVersions** | | Version(s) of parent product if applicable.  If ***ParentProductName*** is N/A, this field contains an empty array. | |
| **ResolutionAvailable** | | Boolean (true, false) . **true** when a resolution is available for the given ***ComponentName***, ***ComponentID, & ComponentVersions***. | |
| **Resolutions** | | Array of vulnerability resolutions | |
| **SolutionInError** | For SMP/E products, this is the SYSMOD or FMID that introduced the SECINT.  For non-SMP/E products, this is the identifier for the patch in error |
| **ErrorReasonID** | Unique reason ID for *Solution in Error* |
| **ErrorDate** | Date solution was placed in Error in ISO 8601 format (yyyy-mm-dd). |
| **ResolutionType** | Patch, Configuration, Upgrade, etc. |
| **ResolutionAvailableDate** | Date when fix first became available in ISO 8601 format (yyyy-mm-dd) |
| **ResolutionID** | For SMP/E products, the resolving PTF  For non-SMP/E products, this is the identifier for the resolving patch |
| **Severity** | This is the software providers rating of the vulnerability severity:  None, Low, Medium, High, Critical | | | |
| **CVSS** | JSON object grouping all CVSS related fields | | | |
| **CVSSVersion** | The CVSS Scoring Version. For example:  1, 2, 3.0, 3.1, 4.0, etc | | |
| **CVSSVector** | The vectors used to score the vulnerability. For example: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:R | | |
| **CVSSURL** | A fully formed URL for the National Vulnerability Database for this Common Vulnerability Scoring System Calculator for this vulnerability. For example:  [https://nvd.nist.gov/vuln-metrics/CVSS/v3-calculator?version=3.1&vector=AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:R](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:R) | | |
| **CVSSScore** | Object of CVSS scores. For example:  { "Overall":"10.0",  "Base":"10.0",  "Temporal":"9.5",  “Environmental: “N/A”} | | |
| **CVE** | Array of public Common Vulnerability and Exposures (CVE) identifiers.  Empty if no CVE is assigned. | | | |
| **SecurityAdvisoryURL** | A fully formed URL for the software suppliers Security Advisory for this vulnerability | | | |
| **WorkaroundAvailable** | Boolean (true, false) | | | |
| **FurtherDetails** | Additional details including workaround instructions. (example – link to a webpage) | | | |
| **LastUpdatedDate** | Date when JSON was last updated in ISO 8601 (yyyy-mm-dd) format. | | | |

SMP/E Sample Enhanced CVSS Data JSON file:

[

{

"DocumentVersion": "1.0",

"Vendor": "Pretend Software, Inc",

"Platform": "zArchitecture",

"OperatingSystem": "z/OS",

“Title”: “PretendOS: Remote Command Execution in pretendFS”,

"InitialPublicationDate": "2024-03-23",

"UniqueIssueIdentifierType": "APAR",

"UniqueIssueIdentifier": "ABC1234",

"ImpactedComponents": [

{

"ComponentType": "Software",

"ComponentName": "Product 1",

"ComponentID": "PROD1001",

"ComponentVersions": ["3.1"],

"ParentProductName": "Parent Product",

"ParentProductVersions": ["3.1"],

"ResolutionAvailable": true,

"Resolutions":

[

{

"SolutionInError"  "PTF or FMID that introduce SECINT",

"ErrorReasonID: : "unique reason ID",

"ErrorDate" : "2024-04-15",

"ResolutionType": "Patch",

"ResolutionAvailableDate": "2024-04-23",

"ResolutionID": "PTF number",

}

]

},

{

"ComponentType": "Software",

"ComponentName": "Product 2",

"ComponentID": "PROD1001",

"ComponentVersions": ["3.1"],

"ParentProductName": "Parent Product 2",

"ParentProductVersions": ["3.1"],

"ResolutionAvailable": false,

"Resolutions": []

},

{

"ComponentType": "Software",

"ComponentName": "Product 3",

"ComponentID": "PROD3001",

"ComponentVersions": ["2.5"],

"ParentProductName": "Parent Product 3",

"ParentProductVersions": ["3.1"],

"ResolutionAvailable": true,

"Resolutions": [

{

"SolutionInError"  "PTF or FMID that introduce SECINT",

"ErrorReasonID: : "unique reason ID",

"ErrorDate" : "2024-04-15",

"ResolutionType": "Patch",

"ResolutionAvailableDate": "2024-04-23",

"ResolutionID": "PTF number",

},

]

},

{

"ComponentType": "Software",

"ComponentName": "Product 3",

"ComponentID": "PROD3001",

"ComponentVersions": ["3.1"],

"ParentProductName": "Parent Product 3",

"ParentProductVersions": ["3.1"],

"ResolutionAvailable": true,

"Resolutions": [

{

"SolutionInError"  "PTF or FMID that introduce SECINT",

"ErrorReasonID: : "unique reason ID",

"ErrorDate" : "2024-04-15",

"ResolutionType": "Patch",

"ResolutionAvailableDate": "2024-04-23",

"ResolutionID": "PTF number 2",

}

]

},

],

"Severity": "Critical",

"CVSS":{

"CVSSVersion": "3.0",

"CVSSVector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C",

"CVSSUrl": [https://nvd.nist.gov/vuln-metrics/CVSS/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C&version=3.0](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C&version=3.0),

"CVSSScore": {

"Overall":"9.5",

"Base":"10.0",

"Temporal":"9.5"

},

},

"CVE": ["CVE-0000-0000"],

"SecurityAdvisoryUrl": <https://pretend_software.com/security-advisories/ABC1234>",

"WorkaroundAvailable": false,

"FurtherDetails": "" ,

"LastUpdatedDate": "2024-04-24"

}

]

Non-SMP/E Sample Enhanced CVSS Data JSON file:

[

{

"DocumentVersion": "1.0",

"Vendor": "Pretend Software, Inc",

"Platform": "zArchitecture",

"OperatingSystem": "z/OS",

"Title": "PretendOS: Remote Command Execution in pretendFS",

"InitialPublicationDate": "2024-03-21",

"UniqueIssueIdentifierType": "Security Notice",

"UniqueIssueIdentifier": "ABC1234",

"ImpactedComponents":

[

{

"ComponentType": "Software",

"ComponentName": "IBM WebSphere Application Server”,

"ComponentID": "N/A",

"ComponentVersions": ["17.0.0.1",

"17.0.0.2",

"18.0.0.6",

"18.0.0.7",

"19.1.0.2",

"19.1.0.3",

"20.0.0.1"],

"ParentProductName": "Parent Product",

"ParentProductVersions": ["3.1"],

"ResolutionAvailable": true,

"Resolutions":

[

{

"SolutionInError"  "PTF or FMID”

"ErrorReasonID: : "unique reason ID",

"ErrorDate" : "2024-04-15",

"ResolutionType": "Upgrade",

"ResolutionAvailableDate": "2024-04-23",

"ResolutionID": "20.0.0.2",

},

{

"SolutionInError"  "PTF or FMID",

"ErrorReasonID: : "unique reason ID",

"ErrorDate" : "2024-04-15",

"ResolutionType": "Patch",

"ResolutionAvailableDate": "2024-04-23",

"ResolutionID": "PH57933",

},

]

},

],

"Severity": "Critical",

"CVSS":{

"CVSSVersion": "3.0",

"CVSSVector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C",

"CVSSUrl": [https://nvd.nist.gov/vuln-metrics/CVSS/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C&version=3.0](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C&version=3.0),

"CVSSScore": {

"Overall":"9.5",

"Base":"10.0",

"Temporal":"9.5"

},

},

"CVE": ["CVE-0000-0000"],

"SecurityAdvisoryURL": https://pretend\_software.com/security-advisories/ABC1234,

"WorkaroundAvailable": false,

"FurtherDetails": ""

"LastUpdatedDate": "2024-04-24"

}

]