Vulnerability Scan Results in XML

Vulnerability scan results may be downloaded in XML format from the scan history list. The vulnerability scan results in XML format contains the same content as the vulnerability scan results in other supported formats (PDF, HTML, MHT and CSV).

The scan results report includes summary and host-based results. The report summary in the header section provides summary information about the scan, including the user who requested the scan, the time when the scan was initiated, the target hosts, and how long the scan took to complete. Host-based results include detailed information on vulnerabilities detected for each scanned host.

The service associates the "scan-1.dtd" with vulnerability scan results XML output. The "scan-1.dtd" describes the markup declarations for the report elements (element types, attribute lists, entities, and notations). This DTD can be found at the API Server URL appropriate for your account location.

Account Location	API Server URL
US Platform	https://qualysapi.qualys.com/scan-1.dtd
EU Platform	https://qualysapi.qualys.eu/scan-1.dtd
@Customer Platform	https://qualysapi.<customerbaseURL>/scan-1.dtd

DTD for Vulnerability Scan Results

A recent "scan-1.dtd" is shown below.

```
<!-- QUALYS SCAN DTD -->

<!ELEMENT SCAN ((HEADER | ERROR | IP)+)>
<!ATTLIST SCAN
    value CDATA #REQUIRED
>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!-- INFORMATION ABOUT THE SCAN -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ELEMENT KEY (#PCDATA)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>
<!-- NAME of the asset group with the TYPE attribute with possible values of
     (DEFAULT | EXTERNAL | ISCANNER) -->
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
<!-- IP -->
<!ELEMENT IP (OS?, OS_CPE?, NETBIOS_HOSTNAME?, INFOS?, SERVICES?, VULNS?, PRACTICES?)>
<!ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    status CDATA #IMPLIED
>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
```

```
<!ELEMENT NETBIOS_HOSTNAME (#PCDATA)>
<!-- CATEGORIES OF INFO, SERVICE, VULN or PRACTICE -->
<!ELEMENT CAT (INFO+ | SERVICE+ | VULN+ | PRACTICE+)>
<!ATTLIST CAT
    value CDATA #REQUIRED
    fqdn CDATA #IMPLIED
    port CDATA #IMPLIED
    protocol CDATA #IMPLIED
    misc CDATA #IMPLIED
>
<!-- IP INFORMATIONS -->
<!ELEMENT INFOS (CAT)+>
<!ELEMENT INFO (TITLE, LAST_UPDATE?, PCI_FLAG, VENDOR_REFERENCE_LIST?,
                CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?, CONSEQUENCE?, SOLUTION?,
                COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST INFO
    severity CDATA #IMPLIED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- MAP OF SERVICES -->
<!ELEMENT SERVICES (CAT)+>
<!ELEMENT SERVICE (TITLE, LAST_UPDATE?, PCI_FLAG, VENDOR_REFERENCE_LIST?,
                   CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?, CONSEQUENCE?, SOLUTION?,
                   COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST SERVICE
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- VULNERABILITIES -->
<!ELEMENT VULNS (CAT)+>
<!ELEMENT VULN (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?, PCI_FLAG,
                VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?,
                CONSEQUENCE?, SOLUTION?, COMPLIANCE?, CORRELATION?, RESULT?)>
<!-- number is Qualys numeric ID -->
<!-- cveid is the CVE identification code (if any) -->
<!-- severity is Qualys severity level 1 to 5 (possibly customized)  -->
<!-- standard-severity is the original Qualys severity level 1 to 5 if it has been
customized by the user -->
<!ATTLIST VULN
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- Required Element -->
<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->
<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>

<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
```

```
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
                           COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!-- if format is set to "table" -->
<!-- tab '\t' is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT
    format CDATA #IMPLIED
>

<!-- SECURITY TIPS -->
<!ELEMENT PRACTICES (CAT+)>
<!ELEMENT PRACTICE (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?, PCI_FLAG,
                    VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?,
                    CONSEQUENCE?, SOLUTION?, COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST PRACTICE
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>
<!-- EOF -->
```

XPaths for Vulnerability Scan Results

This section describes the XPaths in the XML scan results, which includes several sections.

Header Information

HEADER and IP Elements

XPath	element specification / notes
/SCAN	((HEADER | ERROR | IP)+)
attribute: **`value`**	**`value`** is *required* and is the reference number for the scan
/SCAN/HEADER	(KEY+, ASSET_GROUPS?, OPTION_PROFILE?)
/SCAN/HEADER/KEY	(#PCDATA)
attribute: **`value`**	**`value`** is *implied* and, if present, will be one of the following: USERNAME.................. The QualysGuard user login name for the user that initiated the scan request. COMPANY..................... The company associated with the QualysGuard user. DATE.............................. The date when the scan was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" TITLE .... A descriptive title. When the user specifies a title for the scan request, the user-supplied title appears. When unspecified, a standard title is assigned. TARGET.......................... The target host(s). DURATION.................... The time it took to complete the scan. SCAN_HOST .... The host name of the host that processed the scan. NBHOST_ALIVE........... The number of hosts found to be “alive.” NBHOST_TOTAL.......... The total number of hosts. REPORT_TYPE .... The report type: “API” for an on-demand scan request launched from the API, “On-demand” for an on-demand scan launched from the QualysGuard user interface, and “Scheduled” for a scheduled task. OPTIONS........................ The options settings in the options profile that was applied to the scan. Note the options information provided may be incomplete. DEFAULT_SCANNER.. The value 1 indicates that the default scanner was enabled for the scan. ISCANNER_NAME...... The scanner appliance name or “external” (for external scanner) used for the scan.
/SCAN/HEADER/KEY	(#PCDATA)
attribute: **`value`**	STATUS........................... The job status reported for the scan. FINISHED is returned when the scan completed and there were vulnerabilities found. NOVULNSFOUND is returned when the scan completed and no vulnerabilities were found. CANCELED is returned when the scan was canceled. NOHOSTALIVE is returned when the scan completed and the target hosts were down (not alive). PAUSED is returned when a scan was paused. INTERRUPTED is returned when the scan was interrupted and did not complete.
/SCAN/ERROR	(#PCDATA)
attribute: **`number`**	**`number`** is *implied* and, if present, is an error code
/SCAN/HEADER/ASSET_GROUPS	(ASSET_GROUP+)
/SCAN/HEADER/ASSET_GROUPS/ASSET_GROUP	(ASSET_GROUP_TITLE)
/SCAN/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE	(#PCDATA)
	The title of an asset group that was included in the scan target.

HEADER and IP Elements (continued)

XPath	element specification / notes
/SCAN/HEADER/OPTION_PROFILE	(OPTION_PROFILE_TITLE)
/SCAN/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE	(#PCDATA)
	The title of the option profile, as defined in the QualysGuard user interface, that was applied to the scan.
attribute: **option_profile_default**	**option_profile_default** is *implied* and, if present, is a code that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.
/SCAN/IP	(OS?, OS_CPE?, NETBIOS_HOSTNAME?, INFOS?, SERVICES?, VULNS?, PRACTICES?)
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is an Internet DNS host name
attribute: **status**	**status** is *implied* and, if present, will be one of the following: down ....The host was down (appears in live scan results only). Finish ....The scan finished (appears in live scan results only). no vuln ....No vulnerabilities were found on the host (appears in saved scan reports and live scan results). Note: The “down” or “Finish” element appears online in live scan results only, the results returned directly from the scanner. These elements are not present in saved scan reports, retrieved using the scan_report.php function.
/SCAN/IP/OS	(#PCDATA)
	The operating system name detected on the host.
/SCAN/IP/OS_CPE	(#PCDATA)
	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/SCAN/IP/NETBIOS_HOSTNAME	(#PCDATA)
	The NetBIOS host name, when available.

Information Gathered

Information gathered vulnerabilities are grouped under the <INFOS> element.

INFOS Element

XPath	element specification / notes
/SCAN/IP/INFOS	(CAT)+
/SCAN/IP/INFOS/CAT	(INFO+) Note: When CAT is a child of INFOS, it can only contain INFO elements.
attribute: **value**	**value** is *required* and will be one vulnerability category name
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number the information gathered was detected on
attribute: **protocol**	**protocol** is *implied* and, if present, is the protocol used to detect the information gathered, such as TCP or UDP
attribute: **misc**	**misc** is *implied* and, if present, will be “over ssl,” indicating the information gathered was detected using SSL

Services

Services vulnerabilities are grouped under the <SERVICES> element.

SERVICES Element

XPath	element specification / notes
/SCAN/IP/SERVICES	(CAT)+
/SCAN/IP/SERVICES/CAT	(SERVICE+) Note: When CAT is a child of SERVICES, it can only contain SERVICE elements.
attribute: **`value`**	**`value`** is *required* and will be one vulnerability category name
attribute: **`fqdn`**	**`fqdn`** is *implied* and, if present, is the fully qualified Internet host name
attribute: **`port`**	**`port`** is *implied* and, if present, is the port number the service was detected on
attribute: **`protocol`**	**`protocol`** is *implied* and, if present, is the protocol used to detect the service, such as TCP or UDP
attribute: **`misc`**	**`misc`** is *implied* and, if present, will contain “over ssl,” indicating the service was detected using SSL

Confirmed Vulnerabilities

Confirmed vulnerabilities are grouped under the <VULNS> element.

VULNS Element

XPath	element specifications / notes
/SCAN/IP/VULNS	(CAT)+
/SCAN/IP/VULNS/CAT	(VULN+) Note: When CAT is a child of VULNS, it can only contain VULN elements.
attribute: **`value`**	**`value`** is *required* and will be one vulnerability category name
attribute: **`fqdn`**	**`fqdn`** is *implied* and, if present, is the fully qualified Internet host name
attribute: **`port`**	**`port`** is *implied* and, if present, is the port number the confirmed vulnerability was detected on
attribute: **`protocol`**	**`protocol`** is *implied* and, if present, is the protocol used to detect the confirmed vulnerability, such as TCP or UDP
attribute: **`misc`**	**`misc`** is *implied* and, if present, will contain “over ssl,” indicating the confirmed vulnerability was detected using SSL

Potential Vulnerabilities

Potential vulnerabilities are grouped under the <PRACTICES> element.

PRACTICES Element

XPath	element specifications / notes
/SCAN/IP/PRACTICES	(CAT)+
/SCAN/IP/PRACTICES/CAT	(PRACTICE+) Note: When CAT is a child of PRACTICES, it can only contain PRACTICE elements. A practice is a potential vulnerability.
attribute: **`value`**	**`value`** is *required* and will be one vulnerability category name
attribute: **`fqdn`**	**`fqdn`** is *implied* and, if present, is the fully qualified Internet host name
attribute: **`port`**	**`port`** is *implied* and, if present, is the port number the potential vulnerability was detected on
attribute: **`protocol`**	**`protocol`** is *implied* and, if present, is the protocol used to detect the potential vulnerability, such as TCP or UDP
attribute: **`misc`**	**`misc`** is *implied* and, if present, will contain “over ssl,” indicating the potential vulnerability was detected using SSL

Vulnerability Details

Vulnerability details are provided for each detected vulnerability using the vulnerability elements. The details for each vulnerability instance appear under grouping and category elements: confirmed vulnerability (VULNS/CAT/VULN), potential vulnerability (PRACTICES/CAT/PRACTICE), information gathered (INFOS/CAT/INFO), and service (SERVICES/CAT/SERVICE).

Vulnerability Elements

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element	
	(TITLE, LAST_UPDATE, CVSS_BASE?, CVSS_TEMPORAL?, PCI_FLAG, VENDOR_REFERENCE_LIST?, BUGTRAQ_ID_LIST?, CVE_ID_LIST, DIAGNOSIS?, CONSEQUENCE?, SOLUTION?, COMPLIANCE?, CORRELATION?, RESULT?)
	The vulnerability element, where the variable "vulnerability_elements" represents a vulnerability element grouping: VULNS for confirmed vulnerabilities, PRACTICES for potential vulnerabilities, INFOS for information gathered, or SERVICES for services. The variable "vulnerability_element" represents a vulnerability element for a single vulnerability instance: VULN for confirmed vulnerability, PRACTICE for potential vulnerability, INFO for information gathered, or SERVICE for service.
attribute: **`number`**	**`number`** is *required* and is the Qualys ID number assigned to the vulnerability
attribute: **`cveid`**	**`cveid`** is *implied* and, if present, is the CVE ID (name) for the vulnerability
attribute: **`severity`**	**`severity`** is *required* and is the severity level assigned to the vulnerability, an integer between 1 and 5
attribute: **`standard-severity`**	**`standard-severity`** is *implied* and, if present, is the standard severity level assigned to the vulnerability by QualysGuard, an integer between 1 and 5
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/TITLE (#PCDATA)	
	The title of the vulnerability, from the QualysGuard KnowledgeBase.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/LAST_UPDATE (#PCDATA)	
	The date and time when the vulnerability was last updated in the QualysGuard KnowledgeBase, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVSS_BASE (#PCDATA)	
	The CVSS base score assigned to the vulnerability.
attribute: **`source`**	Note: This attribute is never present in XML output for this release.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVSS_TEMPORAL (#PCDATA)	
	The CVSS temporal score assigned to the vulnerability.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/PCI_FLAG (#PCDATA)	
	A flag indicating whether this vulnerability must be fixed to pass a PCI compliance scan. This information helps users to determine whether the vulnerability must be fixed to meet PCI compliance goals, without having to run additional PCI compliance scans. The value 1 is returned when the vulnerability must be fixed to pass PCI compliance; the value 0 is returned when the vulnerability does not need to be fixed to pass PCI compliance.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/DIAGNOSIS (#PCDATA)	
	A description of the threat posed by the vulnerability, from the QualysGuard KnowledgeBase.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CONSEQUENCE (#PCDATA)	
	A description of the impact, or consequences, that may occur if the vulnerability is successfully exploited, from the QualysGuard KnowledgeBase.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/SOLUTION (#PCDATA)	
	A verified solution to fix the vulnerability, from the QualysGuard KnowledgeBase.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE (COMPLIANCE_INFO+)	
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO	
	(COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)

Vulnerability Elements (continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_TYPE	(#PCDATA)
	The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: -HIPAA (Health Insurance Portability and Accountability Act) -GLBA (Gramm-Leach-Bliley Act) -CobIT (Control Objectives for Information and related Technology -SOX (Sarbanes-Oxley Act)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_SECTION	(#PCDATA)
	The section of a compliance policy or regulation associated with the vulnerability.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_DESCRIPTION	(#PCDATA)
	The description of a compliance policy or regulation associated with the vulnerability.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION	(EXPLOITABILITY?,MALWARE?)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY	(EXPLT_SRC)+
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC	(SRC_NAME, EXPLT_LIST)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME	(#PCDATA)
	The name of the third party vendor or publicly available source of the exploitability information.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST	(EXPLT)+
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT	(REF, DESC, LINK?)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF	(#PCDATA)
	The CVE reference for the exploitability information.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC	(#PCDATA)
	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK	(#PCDATA)
	A link to the exploit, when available.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE	(MW_SRC)+
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC	(SRC_NAME, MW_LIST)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/SRC_NAME	(#PCDATA)
	The name of the source of the malware information: Trend Micro.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST	(MW_INFO)+
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO	(MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)

Vulnerability Elements (continued)

XPath	element specifications / notes
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_ID	(#PCDATA)
	The malware name/ID assigned by Trend Micro.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_TYPE	(#PCDATA)
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_PLATFORM	(#PCDATA)
	A list of the platforms that may be affected by the malware.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_ALIAS	(#PCDATA)
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_RATING	(#PCDATA)
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_LINK	(#PCDATA)
	A link to malware details.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/RESULT	(#PCDATA)
	Specific scan test results for the vulnerability, from the host assessment data.
attribute: **`format`**	**`format`** is *implied* and, if present, will be "table" to indicate that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/VENDOR_REFERENCE_LIST	(VENDOR_REFERENCE+)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE	(ID, URL)
	The name of a vendor reference, and the URL to this vendor reference.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/reference_list/reference/ID	(#PCDATA)
	The name of a vendor reference, CVE name, or Bugtraq ID.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/reference_list/reference/URL	(#PCDATA)
	The URL to the vendor reference, CVE name, or Bugtraq ID.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVE_ID_LIST	(CVE_ID+)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/CVE_ID_LIST/CVE_ID	(ID, URL)
	A CVE name assigned to the vulnerability, and the URL to this CVE name. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/BUGTRAQ_LIST	(BUGTRAQ_ID+)
/SCAN/IP/vulnerability_elements/CAT/vulnerability_element/BUGTRAQ_LIST/BUGTRAQ_ID	(ID, URL)
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.