DCE SMB Inspector

DCE SMB Inspector Overview

Type	Inspector (service)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	None
Enabled	`true`

The DCE/RPC protocol allows processes on separate network hosts to communicate as if the processes were on the same host. These inter-process communications are commonly transported between hosts over TCP and UDP. Within the TCP transport, DCE/RPC might also be further encapsulated in the Windows Server Message Block (SMB) protocol or in Samba, an open-source SMB implementation used for inter-process communication in a mixed environment comprised of Windows, and UNIX or Linux operating systems.

Although most DCE/RPC exploits occur in DCE/RPC client requests targeted for DCE/RPC servers, which could be practically any host on your network that is running Windows or Samba, exploits can also occur in server responses.

IP encapsulates all DCE/RPC transports. TCP transports all connection-oriented DCE/RPC, such as SMB.

The `dce_smb` inspector detects connection-oriented DCE/RPC in the SMB protocol and uses protocol-specific characteristics including header length and data fragment order to:

- Detect DCE/RPC requests and responses encapsulated in SMB transports.
- Analyze DCE/RPC data streams and detect anomalous behavior and evasion techniques in DCE/RPC traffic.
- Analyze SMB data streams and detect anomalous SMB behavior and evasion techniques.

- Desegment SMB and defragment DCE/RPC.
- Normalize DCE/RPC traffic for processing by the rules engine.

The following diagram illustrates the point at which the DCE SMB inspector begins processing traffic for the SMB transport.

The `dce_smb` inspector typically receives SMB traffic on the well-known TCP port 139 for the NetBIOS Session Service or the similarly implemented well-known Windows port 445. Because SMB has many functions other than transporting DCE/RPC, the inspector first tests whether the SMB traffic is carrying DCE/RPC traffic and stops processing if it is not, or continues processing if it is.

Descriptions of the `dce_smb` inspector parameters and functionality include the Microsoft implementation of DCE/RPC known as Microsoft Remote Procedure Call (MSRPC), as well as both SMB and Samba.

Target-Based Policies

Windows and Samba DCE/RPC implementations differ significantly. For example, all versions of Windows use the DCE/RPC context ID in the first fragment when defragmenting DCE/RPC traffic, and all versions of Samba use the context ID in the last fragment. As another example, Windows Vista uses the `opnum` (operation number) header field in the first fragment to identify a specific function call, and Samba and all other Windows versions use the `opnum` field in the last fragment.

There are significant differences in Windows and Samba SMB implementations. For example, Windows recognizes the SMB OPEN and READ commands when working with named pipes, but Samba does not recognize these commands.

For this reason, the `dce_smb` inspector uses a target-based approach. When you configure a `dce_smb` inspector instance, the `policy` parameter specifies an implementation of the DCE/RPC SMB protocol. This in combination with the host information establishes a default target-based server policy. Optionally, you can configure additional inspectors that target other hosts and DCE/RPC SMB implementations. The DCE/RPC SMB implementation specified by the default target-based server policy applies to any host not targeted by another `dce_smb` inspector instance.

DCE/RPC SMB implementations which the `dce_smb` inspector can target with the `policy` parameter are:

- WinXP (default)
- Win2000
- WinVista
- Win2003
- Win2008
- Win7
- Samba
- Samba-3.0.37

- Samba-3.0.22
- Samba-3.0.20

File Inspection

The `dce_smb` inspector supports file inspection for SMB versions 1, 2, and 3.

The `dce_smb` inspector examines normal SMB file transfers. This includes checks of the file type and signature through the file processing as well as setting a pointer for the `file_data` rule option. The `dce_smb` inspector supports inspection of normal SMB file transfers for SMB version 1, 2, and 3 when used in coordination with the `file_id` inspector (described in Snort 3 open source documentation, available at https://www.snort.org/snort3). To enable file inspection, configure the `file_id` inspector as needed, and set the `dce_smb` `smb_file_inspection` and `smb_file_depth` parameters. The `smb_file_depth` parameter indicates the number of file data bytes the `file_id` inspector examines beginning at the pointer indicated by the `file_data` IPS rule option. For more information, see the Snort 3 open source documentation, available at https://www.snort.org/snort3).

Defragmentation

The `dce_smb` inspector supports reassembling fragmented data packets. This feature is useful in inline mode to catch exploits early in the inspection process before full defragmentation is done, or to catch exploits that take advantage of fragmentation to conceal themselves. Be aware that disabling defragmentation may result in a large number of false negatives.

DCE SMB Inspector Parameters

DCE SMB port configuration

The `binder` inspector defines the DCE SMB port configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
   {
        "when": {
            "role":"any",
            "service":"netbios-ssn",
            "ports": ""
        },
         "use": {
             "type":"dce_smb"
        }
   }
]
```

max_frag_len

Specifies the maximum fragment length in bytes allowed for defragmentation. For processing larger fragments the inspector considers packet content to this size before defragmenting.

Note The value specified in this parameter must be greater than or equal to the depth to which the rules need to examine the data to ensure detection. To ensure that all data goes through detection, use the default value.

Type: integer

Valid range: `1514` to `65535`

Default value: `65535`

smb_max_compound

Specifies the maximum number of commands to process in one SMB request.

Type: integer

Valid range: `0` to `255`

Default value: `3`

smb_max_chain

Specifies the maximum number of chained SMB AndX commands allowed. Typically, more than a few chained AndX commands represent anomalous behavior and could indicate an evasion attempt. Specify `1` to permit no chained commands or `0` to disable detecting the number of chained commands.

The `dce_smb` inspector first counts the number of chained commands and generates an event if accompanying SMB inspector rules are enabled and the number of chained commands equals or exceeds the configured value. It then continues processing.

You can enable rule 133:20 to generate events and, in an inline deployment, drop offending packets for this parameter.

Type: integer

Valid range: `0` to `255`

Default value: `3`

disable_defrag

Specifies whether to defragment fragmented DCE/RPC traffic. When enabled, the `dce_smb` inspector detects anomalies and sends DCE/RPC data to the rules engine, but at the risk of missing exploits in fragmented DCE/RPC data.

Although `disable_defrag` provides the flexibility of not defragmenting traffic and can speed processing, most DCE/RPC exploits attempt to take advantage of fragmentation to hide the exploit. Enabling this parameter would bypass most known exploits, resulting in a large number of false negatives.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

limit_alerts

Specifies whether to limit the DCE alerts to at most one per signature per flow.

Type: boolean

Valid values: `true`, `false`

Default value: `true`

reassemble_threshold

Specifies the minimum number of bytes in the DCE/RPC desegmentation and defragmentation buffers to queue before sending a reassembled packet to the rules engine. This parameter is useful in inline mode so as to potentially catch an exploit early before full defragmentation is done.

Note that a low value increases the likelihood of early detection but could have a negative impact on performance. You should test for performance impact if you enable this parameter.

A value of `0` disables reassembly.

Type: integer

Valid range: `0` to `65535`

Default value: `0`

policy

Specifies the Windows or Samba DCE/RPC implementation used by the targeted host or hosts on your monitored network segment.

Type: enum

Valid values: A string selected from the following list: `Win2000`, `WinXP`, `WinVista`, `Win2003`, `Win2008`, `Win7`, `Samba`, `Samba-3.0.37`, `Samba-3.0.22`, `Samba-3.0.20`

Default value: `WinXP`

smb_max_credit

Specifies the maximum number of outstanding requests.

Type: integer

Valid range: `1` to `65536`

Default value: `8192`

smb_file_depth

Specifies the number of bytes inspected when a file is detected in SMB traffic, beginning at the location specified by the `file_data` IPS rule option (described in Snort 3 open source documentation, available at https://www.snort.org/snort3).

Specify `-1` to disable file inspection.

Specify `0` to indicate unlimited file inspection.

Type: integer

Valid range: `-1` to `32767`

Default value: `16384`

When a file is detected in SMB traffic, the `smb_file_depth` parameter indicates the number of file data bytes the inspector will examine beginning at the pointer set in the `file_data` IPS rule option. To inspect the file type and signature, `dce_smb` uses the `enable_type`, `type_depth`, `enable_signature`, and `signature_depth` parameters set in the `file_id` inspector. For more information on the `file_id` inspector, see the Snort open source documentation, available at https://www.snort.org/snort3.

memcap

Specifies the maximum memory limit in bytes allocated to the inspector. When the maximum memory cap is reached or exceeded, the `dce_smb` inspector deletes the least recently used data to create more space.

Type: integer

Valid range: `512` to `9,007,199,254,740,992 (maxSZ)`

Default value: `8,388,608`

smb_fingerprint_policy

Causes the inspector to detect the Windows or Samba version that is identified in SMB `Session Setup AndX` requests and responses. When the detected version is different from the Windows or Samba version configured for the `policy` inspector parameter, the detected version overrides the configured version for that session only.

For example, if you set `policy` to Windows XP and the inspector detects Windows Vista, the inspector uses a Windows Vista policy for that session. Other settings remain in effect.

Type: enum

Valid values: `none`, `client`, `server`, or `both`

- Use `client` to inspect server-to-client traffic for the policy type.
- Use `server` to inspect client-to-server traffic for the policy type.
- Use `both` to inspect server-to-client and client-to-server traffic for the policy type.
- Use `none` to disable Windows or Samba version inspection.

Default value: `none`

smb_legacy_mode

When `smb_legacy_mode` is `true`**,** the system applies SMB intrusion rules only to SMB Version 1 traffic, and applies DCE/RPC intrusion rules to DCE/RPC traffic using SMB Version 1 as a transport.

When `smb_legacy_mode` is `false`, the system applies SMB intrusion rules to traffic using SMB Versions 1, and 2, and:

- For Versions 7.0 and 7.0.x the system applies DCE/RPC intrusion rules to DCE/RPC traffic using SMB as a transport only for SMB Version 1.
- For Versions 7.1+ the system applies DCE/RPC intrusion rules to DCE/RPC traffic using SMB as a transport for SMB Versions 1 and 2.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

valid_smb_versions

Specifies which SMB versions to inspect. Separate multiple SMB versions with a space character.

Type: string

Valid values: `v1`, `v2`, `v3`, `all`

Default value: `all`

DCE SMB Inspector Rules

Enable the `dce_smb` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 1: DCE SMB Inspector Rules

GID:SID	Rule Message
133:2	SMB - bad NetBIOS session service session type
133:3	SMB - bad SMB message type
133:4	SMB - bad SMB Id (not \xffSMB for SMB1 or not \xfeSMB for SMB2)
133:5	SMB - bad word count or structure size
133:6	SMB - bad byte count
133:7	SMB - bad format type
133:8	SMB - bad offset
133:9	SMB - zero total data count
133:10	SMB - NetBIOS data length less than SMB header length
133:11	SMB - remaining NetBIOS data length less than command length
133:12	SMB - remaining NetBIOS data length less than command byte count
133:13	SMB - remaining NetBIOS data length less than command data size
133:14	SMB - remaining total data count less than this command data size
133:15	SMB - total data sent (STDu64) greater than command total data expected
133:16	SMB - byte count less than command data size (STDu64)
133:17	SMB - invalid command data size for byte count
133:18	SMB - excessive tree connect requests with pending tree connect responses
133:19	SMB - excessive read requests with pending read responses
133:20	SMB - excessive command chaining

GID:SID	Rule Message
133:21	SMB - multiple chained login requests
133:22	SMB - multiple chained tree connect requests
133:23	SMB - chained/compounded login followed by logoff
133:24	SMB - chained/compounded tree connect followed by tree disconnect
133:25	SMB - chained/compounded open pipe followed by close pipe
133:26	SMB - invalid share access
133:44	SMB - invalid SMB version 1 seen
133:45	SMB - invalid SMB version 2 seen
133:46	SMB - invalid user, tree connect, file binding
133:47	SMB - excessive command compounding
133:48	SMB - zero data count
133:50	SMB - maximum number of outstanding requests exceeded
133:51	SMB - outstanding requests with same MID
133:52	SMB - deprecated dialect negotiated
133:53	SMB - deprecated command used
133:54	SMB - unusual command used
133:55	SMB - invalid setup count for command
133:56	SMB - client attempted multiple dialect negotiations on session
133:57	SMB - client attempted to create or set a file’s attributes to readonly/hidden/system
133:58	SMB - file offset provided is greater than file size specified
133:59	SMB - next command specified in SMB2 header is beyond payload boundary

DCE Inspectors Intrusion Rule Options

dce_iface

Specifies the following comma-separated elements:

- The UUID for a service interface.
- The interface version (optional). The default setting matches any version.

- An indicator of whether a rule should match on any fragment in a request (optional). The default setting matches only the first fragment.

In the DCE/RPC protocol, a client must bind to a service before making a call to it. When a client sends a bind request to the server, it can specify one or more service interfaces to bind to. Each interface is represented by a UUID, and each interface UUID is paired with a unique index (or context ID) that future requests can use to reference the service that the client is calling. The server responds with the interface UUIDs it accepts as valid and allows the client to make requests to those services. When a client makes a request, it will specify the context ID so the server knows to what service the client is making a request.

Using the `dce_iface` rule option, a rule can ask the inspector whether the client has bound to a specific interface UUID and whether this client request is making a request to that interface. This can eliminate false positives where more than one service is bound to successfully since the inspector can correlate the bind UUID to the context id used in the request.

The `dce_iface` option requires tracking client Bind and Alter Context requests as well as server Bind Ack and Alter Context responses for connection-oriented DCE/RPC in the inspector. For each Bind and Alter Context request, the client specifies a list of interface UUIDs along with a handle (or context id) for each interface UUID that will be used during the DCE/RPC session to reference the interface. The server response indicates which interfaces it allows the client to make requests to—it either accepts or rejects the client's wish to bind to a certain interface. This tracking is required so that when a request is processed, the context id used in the request can be correlated with the interface UUID for which it is a handle.

The `dce_iface` rule option matches if:

- the specified interface UUID matches the interface UUID (as referred to by the context ID) of the DCE/RPC request

and

- the `version` argument is not supplied, or the `version` argument is supplied and matches the interface UUID of the DCE/RPC request

and

- the `any_frag` argument is supplied, or the `any_frag` argument is absent and the `dce_iface` option matches the UUID and version criteria on the initial request fragment

Examples:

```
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188, <2;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188,any_frag;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188, =1, any_frag;
```

dce_iface.uuid

A DCE/RPC request can specify whether UUID numbers are represented as big endian or little endian. The representation of the interface UUID in a request is different depending on the endianness specified in the request. The `dce_rpc` inspector normalizes the UUID. This means that the UUID specification in the `dce_iface` rule option must be written the same way regardless of the endianness of the request.

For example, a little endian Bind request would represent a UUID as follows:

```
|f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc|
```

and a big-endian Bind request would represent the same UUID as follows:

```
|5a 7b 91 f8 ff 00 11 d0 a9 b2 00 c0 4f b6 e6 fc|
```

In Snort 3 rules using the `dce_iface` option, the UUID must be represented in a string using big endian order regardless of the endian-ness of the request:

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

Type: string

Syntax: `dce_iface: <UUID>;`

Valid values: Where: *`UUID`* is 32 hexadecimal digits, displayed in five groups separated by hyphens, in the form: `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`

Examples: `dce_iface: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc;`

dce_iface.version

A service interface has a version associated with it. Some versions of an interface may not be vulnerable to certain exploits. For this reason you can specify one or more version numbers in the `dce_iface` option, to determine whether it is necessary to check for a particular exploit.

Type: interval

Syntax: `dce_iface: <range_operator><positive integer>;` or `dce_iface: <positive integer><range_operator><positive integer>;`

Valid values: A set of one or more positive version numbers and a `range_operator` as specified in the Table 2: Range Formats.

Examples: `dce_iface: =6;`

dce_iface.any_frag

A DCE/RPC request can be broken up into one or more fragments. Flags are set in the DCE/RPC header to indicate whether the current fragment is the first, a middle, or the last fragment of the request. Many checks for data in the DCE/RPC request are relevant only if the DCE/RPC request is a first fragment (or full request). Thus, fragments that follow the first fragment contain data deeper into the DCE/RPC request. For example, a rule that looks for data in the first five bytes of the request (for example, a length field), finds the wrong data on a fragment other than the first. The start of subsequent fragments is offset some length from the beginning of the request. This can be a source of false positives in fragmented DCE/RPC traffic.

For this reason, by default the DCE_RPC inspector matches only the initial fragment in a request. To force the inspector to examine all fragments in a request for a match, add `any_frag` to the `dce_iface` rule option. Note that a defragmented DCE/RPC request is considered a full request.

Syntax: `dec_iface: any_frag;`

Examples: `dce_iface: any_frag;`

dce_opnum

Match a DCE RPC operation number, range of operation number, or list of operation number. This option represents one or more a specific function calls that can be made to an interface. After a client has bound to a specific service interface and makes a request to it, rules need to determine what function call the client is making to the service, to check for exploits that may lie within the function call. The functions call(s) are specified as a double-quote-enclosed list of operation numbers (opnums)

Type: string

Syntax: `dce_opnum: <opnum_list>;`

Where *`opnum_list`* is one of the following:

- A single integer.
- A comma-separated list of integers.
- A range of integers specified with a hyphen separating the lowest and highest numbers in the range.
- A combination of the above.

Valid values: A list of DCE/RPC request opnums.

Examples:

```
dce_opnum: "15";
dce_opnum: "15-18";
dce_opnum: "15, 18-20";
dce_opnum: "15, 17, 20-22";
```

dce_stub_data

This option places the detection cursor (used to traverse the packet payload in rules processing) at the beginning of the DCE/RPC stub data, regardless of preceding rule options. This option matches if there is DCE/RPC stub data present.

Syntax: `dce_stub_data;`

Examples: `dce_stub_data;`

Table 2: Range Formats

Range Format	Operator	Description
`operator i`		
	<	Less than
	>	Greater than
	=	Equal
	≠	Not equal
	≤	Less than or equal
	≥	Greater than or equal
`j operator k`		
	<>	Greater than j and less than k
	<=>	Greater than or equal to j and less than or equal to k