

# [NT] Exchange Calendar MODPROPS DoS (MS07-026)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00021.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 10 May 2007 16:09:43 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Exchange Calendar MODPROPS DoS (MS07-026)

---

## SUMMARY

Determina Security Research has discovered a denial of service vulnerability in the code responsible for parsing iCal email attachments in Microsoft Exchange. This vulnerability can be exploited by a malicious email message and results in a denial of service. The vulnerable code is present in Exchange 2000 and 2003.

Microsoft fixed a related vulnerability with the MS06-019 security update, but their fix introduced a new denial of service bug. Determina Security Research was able to develop a proof-of-concept exploit that works against fully-patched Exchange servers.

## DETAILS

The iCal file format is described in detail in RFC2445. The file consists of a series of records, delimited by BEGIN and END tags. Each record can have multiple named properties. The iCal parser in Exchange maintains a table of properties valid in the current context and switches to the appropriate table upon entering a new record.

## [NT] Exchange Calendar MODPROPS DoS (MS07-026)

The X-MICROSOFT-CDO-MODPROPS property is an undocumented Microsoft extension which allows the iCal file to specify a list of properties that are considered valid in a specific record. All other properties will be ignored by Exchange. The following example shows a typical usage of this feature:

```
BEGIN:VEVENT
X-MICROSOFT-CDO-MODPROPS:BEGIN,DTEND,DTSTART,END
DTSTART:19970714T170000Z
DTEND:19970715T035959Z
SUMMARY:Bastille Day Party
END:VEVENT
```

In this example, the SUMMARY property will not be processed by Exchange.

When the parser encounters the MODPROPS property, it calls `CICalSchema::AllocPropTables` to allocate a new table of valid properties. The pointer to the new table is stored in `this->field_F0` and the list of valid properties is copied into the table. If there is a second MODPROPS property, the function will be called again and will reuse the previously allocated table. If the second MODPROPS element is longer than the first one, the copy loop will write past the end of the table.

This vulnerability was fixed in MS06-019 by adding a call to `CICalSchema::FreePropTables` in the beginning of the `AllocPropTables` function. This ensures that the previous property table is freed and `AllocPropTables` allocates a new one of sufficient size.

Unfortunately, `FreePropTables` also sets the `this->field_28` pointer to NULL. The NULL pointer is later used in a `memcpy` operation in `AllocPropTables` and causes an unhandled exception, resulting in a crash of Exchange.

```
// Allocate a new property table

int CICalSchema::AllocPropTables(arg_0, arg_4)
{
    this->FreePropTables();
    ...

    // Allocate space for the new table

    if (this->field_F0 == NULL)
        this->field_F0 = new(vector_size*16);
    ...

    // NULL pointer dereference of this->field_28
    memcpy(&this->field_F4[offset_F4], &this->field_28[index*20], 20);
}
```

[NT] Exchange Calendar MODPROPS DoS (MS07-026)

```
// Free the property table

void CICalSchema::FreePropTables()
{
if (this->field_F0 != NULL) {
...

ExFree(this->field_F0);
this->field_F0 = NULL;
}

if (this->field_F4 != NULL) {
if (this->field_28 == this->field_F4) {
this->field_28 = NULL; // set this->field_28 to NULL
this->field_1C = 0;
}

ExFree(this->field_F4);
this->field_F4 = NULL;
}

...
}
```

Vendor response:  
Microsoft issued the MS07-026 patch on May 8, 2007.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:asotirov@xxxxxxxxxxxxxx>>  
Alexander Sotirov.  
The original article can be found at:  
<<http://www.determina.com/security.research/vulnerabilities/exchange-ical-modprops.html>>  
<http://www.determina.com/security.research/vulnerabilities/exchange-ical-modprops.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.