You Have One New Appwntment - Hacking Proprietary iCalendar Properties

Eugene Lim, Government Technology Agency of Singapore
Eugene Lim
@spaceraccoonsec
Cyber Security Group, Government Technology Agency of Singapore
How often do you get this?
What if it did this?
VMware Boxer CVE-2022-22944
Synology Calendar CVE-2022-22682
Apple Calendar PATCHED (Monterey 12.4)
Microsoft Outlook RESOLVED
Google Calendar BOUNTY
Nextcloud Calendar CVE-2022-24838 CVE-2022-31014
It all began in 1998...
Today’s plan

You Have One New Appointment

- iCalendar Background
- Standard Implementation
- Proprietary Extensions
- Protocol Interactions
- Takeaways
Background on iCalendar Standard
Relevant RFCs

- RFC 5545 (2009) - Desruisseaux (Oracle)
  Internet Calendaring and Scheduling Core Object Specification (iCalendar)

- RFC 5546 (2009) - Daboo (Apple)
  iCalendar Transport-Independent Interoperability Protocol (iTIP)

- RFC 7986 (2016) - Daboo (Apple)
  New Properties for iCalendar

Also RFC6868, RFC7529, RFC7953, RFC9073, RFC9074...
BEGIN:VCALENDAR
VERSION:2.0
PRODID:-//ZContent.net//Zap Calendar 1.0//EN
CALSCALE:GREGORIAN
METHOD:PUBLISH
BEGIN:VEVENT
SUMMARY:Abraham Lincoln
UID:c7614cfe-3549-4a00-9152-d25cc1fe077d
SEQUENCE:0
STATUS:CONFIRMED
TRANSP:TRANSPARENT
RRULE:FREQ=YEARLY;INTERVAL=1;BYMONTH=2;BYMONTHDAY=12
DTSTART:20080212
DTEND:20080213
DTSTAMP:20150421T141403
CATEGORIES:U.S. Presidents
LOCATION:Hodgenville\, Kentucky
GEO:37.5739497; -85.7399606
DESCRIPTION:Born February 12\, 1809\nSixteenth
URL:http://americanhistorycalendar.com/abraham-lincoln
END:VEVENT
END:VCALENDAR
Proprietary extensions = more features!
Proprietary extensions = more features!
Insecure Implementations of Standard RFC Properties
Property Name: DESCRIPTION

Purpose: This property provides a more complete description of the calendar component than that provided by the "SUMMARY" property.

Value Type: TEXT

Example:

DESCRIPTION: Meeting to provide technical review for "Phoenix" design.
Happy Face Conference Room. Phoenix design team MUST attend this meeting.
RSVP to team leader.
Vendors implement this very differently.

Plain Text
- Apple
- Microsoft

HTML
- Google
- VMware
Automatic payload delivery!

You Have One New Appointment

- Email ICS Attachment
- Client adds to calendar
- Trigger payload
Multiple client versions add to the mess.

VMware Boxer iOS 🕷️  
VMware Boxer Android ✅
Apple’s weird parsing...

DESCRIPTION:----- (FaceTime)-----

[FaceTime] nhttps://facetime.apple.com/join#v=1&p=...&k=...

===

---
Please sir, can I have a custom URI exploit?

DESCRIPTION:----( FaceTime )----
\n[FaceTime]\nFile:///System/Applications/Calculator.app\n------
Property Name: ATTENDEE

Purpose: This property defines an "Attendee" within a calendar component.

Value Type: CAL-ADDRESS

Example:

ATTENDEE;MEMBER="mailto:DEV-GROUP@example.com":mailto:joecool@example.com

The value is a URI... the value MUST be a mailto URI, as defined by RFC2368.
Don’t assume anything!

"<script>alert();</script>"@evil.hax

✅ RFC approved!
You Have One New Appoinment
Useful for red teams.
Vulnerable Proprietary Extensions to iCalendar

You Have One New Appointment
A "standard mechanism for doing non-standard things".

X-NON-STANDARD-PROPERTY

No registration authority = wild wild west
The bad old days.

X-MS-OLK-AUTOSTARTCHECK: Specifies whether or not to automatically start the conferencing application when a reminder for the meeting fires.

X-MS-OLK-COLLABORATEDOC: Specifies the path to the conferencing collaboration document.
You Have One New Appointment

2022
Zombie properties still exist.

X-MS-OLK-MWSURL: Specifies the URL of the Meeting Workspace.

Bypasses URI checks but too early for Follina 😎
Google patented a way to iframe widgets...

US20150169528A1 Calendar information events
You Have One New Appointment

We love loading remote content!

BEGIN:VCALENDAR
BEGIN:VEVENT
DTSTART:VALUE=DATE:20060704
DTEND:VALUE=DATE:20060705
SUMMARY:Independence Day
X-GOOGLE-CALENDAR-CONTENT-TITLE:Independence Day
X-GOOGLE-CALENDAR-CONTENT-ICON:http://www.google.com/google-favicon.ico
X-GOOGLE-CALENDAR-CONTENT-WIDTH:276
X-GOOGLE-CALENDAR-CONTENT-HEIGHT:120
X-GOOGLE-CALENDAR-CONTENT-URL:http://www.google.com/logos/july4th06.html
X-GOOGLE-CALENDAR-CONTENT-TYPE:text/html
END:VEVENT
Classics never die.
Apple jerry-rigged its own data structures onto iCalendar.

X-APPLE-SUGGESTION-INFO-UNIQUE-
KEY:|2|\|flightA2\\\|SFO\\\|JFK\\\|A242\\\|DUMMY|\|18\|\\\|com.apple.Safari\\\|AC4EB118-B1B3-4743-9B07-0B53C9FD5112
X-APPLE-STRUCTURED-LOCATION;VALUE=URI;X-ADDRESS="San Francisco, CA 94128, United States";X-APPLE-MAPKIT-HANDLE=CAES/gEirkQpMwb6...;X-APPLE-REFERENCEFRAME=0;X-TITLE=San Francisco International Airport:geo:37.616458,-122.385678
X-APPLE-END-LOCATION;VALUE=URI;X-ADDRESS="John F. Kennedy International Airport, Jamaica, NY 11430, United States";X-APPLE-MAPKIT-HANDLE=CAES2AI...;X-TITLE=John F. Kennedy International Airport:geo:40.643575,-73.782034
X-APPLE-STRUCTURED-DATA:YnBsaXN0MDDUAAEAAgADAAQABQAGAAAcAClgkdmVyc2lvbkkkY...

Decodes to binary property list NSKeyedArchiver format!
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
.plist version="1.0">
<dict>
    <key>SGEventMetadataKey</key>
    <dict>
        <key>SGEventMetadataBundleIdKey</key>
        <string>com.apple.Safari</string>
        <key>SGEventMetadataCategoryDescriptionKey</key>
        <string>Flight</string>
        <dict>
            <key>@type</key>
            <string>http://schema.org/PostalAddress</string>
            <key>addressCountry</key>
            <string>United States</string>
            ...
    </dict>
</dict>
Interactions with SMTP and CalDAV
What happens when you accept the invitation?
iCalendar interacts with SMTP.

Accept invitation

Send email with ICS attachment via SMTP

Calendar server parses acceptance

ATTENDEE;PARTSTAT=ACCEPTED;CN=Eugene Lim:mailto:<ATTENDEE EMAIL>
What could go wrong?

You Have One New Appointment

ORGANIZER;CN=Attacker:mailto:b@a.com

User accepts invitation; Calendar client sends email

EHLO mailserver.com
MAIL FROM "target@user.com"
RCPT TO "b@a.com"

How about newlines?

@securinti
Still a valid email btw...

User accepts invitation; Calendar client sends email

ORGANIZER;CN=Attacker:mailto:b(\nEHLO a\n)a.com

EHLO mailserver.com
MAIL FROM "target@user.com"
RCPT TO "b(EHLO a
EHLO a)
a.com"

SMTP command injection!

@securinti

Nice one!
Impact depends on SMTP server support.
When API fails, try CALDAV?

- Google: Deprecating
- Microsoft: Transition to Graph
- Lark Suite: Read-Only
Future Steps and Takeaways
The evolution of iCalendar is more jerry-rigging 😞
Standardize your own parsing internally?
9. Security Considerations

In addition to the security properties of iCalendar (see Section 7 of [RFC5545]), a "VALARM", if not monitored properly, can be used to disturb users and/or leak personal information. For instance, an undesirable audio alert could cause embarrassment; an unwanted display alert could be considered an annoyance; or an email alert could be used to leak a user's location to a third party or to send unsolicited email to multiple users. Therefore, CalDAV clients and servers that accept iCalendar data from a third party (e.g., via iCalendar Transport-Independent Interoperability Protocol (iTIP) [RFC5546], a subscription feed, or a shared calendar) SHOULD remove each "VALARM" from the data prior to storing in their calendar system.

Security considerations related to unique identifiers for "VALARM" are discussed in Section 4.
Stay frugal with non-standard behavior.
There’s still lots more properties to research!

spaceraccoon.github.io/icalendardb
Thank you!

Eugene Lim
@spacetacoonsec
spacetacoon.dev