SOLUÇÕES SAST: Agora membro do Pathlock Group

COM LINHA DE CABEÇALHO – NÃO É SIMPLESMENTE OBSOLETO; É UM RISCO.

4 DE ABRIL DE 2018 | BLOG DE SEGURANÇA

A adição "WITH HEADER LINE" foi tecnicamente desnecessária voltando várias versões do SAP agora. Isso ocorre porque a instrução declara tabelas internas e um objeto de dados adicional – a linha de cabeçalho.

Há um grande número de notas que divulgam que o uso dessa declaração causa vários problemas de conteúdo. Entre outras coisas, o uso do mesmo nome significa que não é imediatamente aparente se você está trabalhando em uma tabela ou em uma linha de cabeçalho.

No entanto, o que as notas normalmente não avisam é que esse tipo de programação anda de mãos dadas com problemas de segurança para seus sistemas SAP.

Apesar de tudo, as linhas de cabeçalho ainda podem ser encontradas em grande parte do código do programa. O argumento típico é que usar uma linha de cabeçalho é a única maneira de usar formulários curtos. Isso garante que a estrutura a ser adicionada não precise mais ser especificada explicitamente.

Exemplo:

Report ZEXAMPLE_HEADERLINE

```
1  REPORT  zexample_headerline.
2
3  DATA: it TYPE sflight OCCURS 0 WITH HEADER LINE.
4
5  it-carrid = 'AA'.
6  it-connid = '0700'.
7  APPEND it.        "<- shortened notation
```

Como isso se torna um risco de segurança para seus sistemas SAP

Os sistemas SAP também são compatíveis com Unicode há muito tempo, o que permite que outros scripts não latinos sejam usados. Todos os scripts são considerados equivalentes e podem ser usados em paralelo. Isso significa que um usuário não pode reconhecer se a letra no SAP está em alfabeto latino ou cirílico.

Além disso, todas as versões do SAP usam a tabela "TRMAC" há muitos anos. Esta tabela é usada para ter macros globais SAP disponíveis para encurtar o código.

Se as três opções (forma abreviada + habilitado para Unicode + tabela "TRMAC") forem combinadas, agora é possível ocultar o código com eficácia.

Por exemplo, o código criado no TRMAC é semelhante ao formato curto. No entanto, a primeira letra é substituída por seu equivalente cirílico. Mesmo desenvolvedores experientes normalmente não notam imediatamente a mudança no código ao visualizar a tabela TRMAC com a transação "SM30".

TRMAC

Change View "Macros in ABAP/4 programs": Overview

New Entries

Name of macro	Line	Macro text
APPEND	0000	WRITE: / 'You have been pwned'
APPEND	0001	APPEND &1

Código

Report ZEXAMPLE_HEADERLINE

```
1  REPORT  zexample_headerline.
2
3  DATA: it TYPE sflight OCCURS 0 WITH HEADER LINE.
4
5  it-carrid = 'AA'.
6  it-connid = '0700'.
7  APPEND it.        "<- Macro from TRMAC
```

Apesar disso, o programa executa a macro e continua rodando sem nenhum erro visível:

```
Example for the Headerline

You have been pwned
```

A única diferença visível está no editor: as palavras-chave são codificadas por cores, mas as macros não. Muitos desenvolvedores geralmente consideram as palavras-chave que não são codificadas por cores como algo para o qual nenhuma alteração foi feita e, portanto, elas caem nas racha duras.

Mesmo que o código correspondente seja pesquisado usando "APEND", você o encontrará apenas copiando a macro da tabela TRMAC e colando-a no campo de pesquisa. A tabela interna mais conhecida com uma linha de cabeçalho (que ainda é usada hoje) é a tabela SCREEN, na qual você pode editar campos dynpro antes de exibi-los. O exemplo acima também funciona com isso.

Como proteger seus sistemas SAP do código ABAP oculto

Use apenas código escrito corretamente e evite versões abreviadas. Isso significa que a estrutura deve ser especificada explicitamente e mais palavras serão incluídas na instrução.

Assegure-se de que sejam necessárias definições para variáveis adicionais. Os desenvolvedores são muito mais propensos a notar variáveis denominadas "FROM", "INTO" ou "TO" em seu código de programa, especialmente se a verificação de sintaxe avançada for executada:

Report ZEXAMPLE_HEADERLINE

```
1  REPORT  zexample_headerline.
2
3  DATA: it TYPE STANDARD TABLE OF sflight,
4        wa TYPE sflight.
5  wa-carrid = 'AA'.
6  APPEND wa TO it.     "<- TO comes in addition
```

O uso da tabela SCREEN com a notação abreviada tornou-se obsoleto desde algumas versões do SAP. Portanto, use a seguinte sintaxe:

```
DATA: ls_screen TYPE screen.

LOOP AT SCREEN INTO ls_screen.

  MODIFY SCREEN FROM ls_screen.
ENDLOOP.
```

MARKUS REST

DESENVOLVIMENTO SAP ABAP

Você está ansioso por mais dicas e recomendações na área de SAP Security and Compliance? Existem muitas oportunidades de se envolver conosco – em um de nossos webinars , por exemplo.

compartilhar twitter compartilhar compartilhar e-mail

PUBLICADO EM SEGURANÇA SAP

CIBER SEGURANÇA | SEGURANÇA SAP | DETECÇÃO DE AMEAÇAS

« SEUS CUSTOS DE LICENCIAMENTO SAP SÃO REALMENTE OTIMIZADOS?

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS – SUA PROTEÇÃO ESTÁ EM VIGOR? »

Procurar …

VISITE O BLOG DO PATHLOCK

pathlock

TÓPICOS

- Geral (13)
- Referências e Melhores Casos (16)
- Autorizações SAP e GRC (38)
- Serviços Gerenciados SAP (5)
- Segurança SAP (32)
- Detecção de Ameaças SAP (23)
- SAST SUITE (19)

LINKS

- Blogue (alemão)
- Site da Pathlock Deutschland
- Twitter
- LinkedIn
- XING